La criptografía cuántica una tecnología clave para la seguridad de red

Javier y Ana Areitio Bertolín

Prof. Dr. Javier Areitio Bertolín
jareitio@eside.deusto.es
Catedrático de la Facultad de Ingeniería. ESIDE. Director del Grupo de Investigación Redes y Sistemas. Universidad de Deusto (UD).

Prof. Dra. Ana Areitio Bertolín
ana.areitio@ehu.es.
Laboratorio de Informática Aplicada. Universidad del País Vasco (UPV/EHU).

En el presente artículo se analiza y evalúa la criptografía cuántica una tecnología que aplica la parte de la física moderna denominada mecánica cuántica en criptografía utilizando fotones polarizados de forma controlada, transmitidos sobre fibra óptica o bien de forma inalámbrica a través de la atmósfera o vía satélite. Una de las implantaciones de la criptografía cuántica a nivel internacional es la red DARPA Quantum Network en la que participan BBN Technologies (http//:www.bbn.com), QinetiQ y las Universidades de Harvard y Boston, esta basada en fibra óptica y utiliza criptografía cuántica para proteger las comunicaciones intercambiadas; integra diez nodos y funciona desde 2004 en Massachusetts.

Así mismo, para proteger las comunicaciones electrónicas, las pasadas elecciones del 21 de Octubre del 2007 en Ginebra (Suiza) se utilizó la criptografía cuántica en la línea de comunicaciones dedicada empleada para contabilizar los votos, para ello se implantó tecnología y componentes de la empresa id Quantique (Ginebra-Suiza; http://www.idquantique.com).

Actualmente se observa un gran crecimiento de este tipo de tecnología en numerosos sectores de la sociedad donde la seguridad es un requisito crítico a tener en cuenta. Cada vez más empresas gastan recursos y poseen programas de investigación activos en sistemas de seguridad basados en criptografía cuántica como HP, IBM, Toshiba, Mitsubishi, Siemens, ARC (Austrian Research Center), NEC y NTT (Nippon Telegraph and Telephone de Japón).

La *criptografía cuántica* es una tecnología que utiliza los principios de la mecánica cuántica para desarrollar criptosistemas que permiten a dos entidades o partes A y B compartir cadenas aleatorias de qubits que pueden utilizarse como clave en un proceso de cifrar o descifrar mensajes transmitidos entre ellos. La característica más importante de la criptografía cuántica es que posibilita detectar si una tercera parte intenta interceptar la clave criptográfica. Como los bits cuánticos no pueden copiarse, si la entidad A envía la clave a la entidad B y una entidad E (que realiza una escucha clandestina) intenta obtener conocimiento de la clave, entonces E corromperá los qubits debido a que de acuerdo a la mecánica cuántica un sistema cuántico no puede medirse sin perturbarlo. Si un escucha clandestino E intenta interceptar el mensaje transmitido entre A y B será detectado. La distribución cuántica de claves o QKD (Quantum Key Distribution) es efectiva debido al teorema de no clonación. Si la entidad E intenta diferenciar entre dos estados no ortogonales, no es posible obtener información sin colapsar el estado de al menos uno de ellos.

Sean $|w\rangle$ y $|z\rangle$ dos estados cuánticos no ortogonales que la entidad E intenta conocer, si estos estados interactúan con un estado estándar $|u\rangle$, entonces: $|w\rangle|u\rangle$ pasa a: $|w\rangle|v\rangle$; además: $|z\rangle|u\rangle$ pasa a: $|z\rangle|v'|$.

La entidad E debería querer que: $|v\rangle$ y $|v'\rangle$ sean diferentes, para conocer la identidad del estado, sin embargo, los productos internos se conservan bajo transformaciones unitarias y:

$$\langle v|v'\rangle\langle w|z\rangle = \langle u|v\rangle\langle w|z\rangle \text{ ó}$$
$$\langle v|v'\rangle = \langle u|u\rangle = 1$$

De modo que $|v\rangle$ y $|v'\rangle$ deben ser idénticas y la entidad E necesitará perturbar uno de los dos estados para adquirir algo de información.

Diferencias entre criptografía moderna y cuántica

Los criptosistemas modernos no cuánticos han sido comprobados durante las pasadas décadas y se han aplicado para la seguridad de las comunicaciones electrónicas. Por ejemplo, los criptosistemas RSA, ElGamal y ECC están actualmente en uso y puede probarse que teóricamente cada uno de estos criptosistemas puede ser atacado/criptoanalizado. Algunos de estos algoritmos son seguros en términos de la gran cantidad de esfuerzo computacional necesario para romperlos que hoy en día esta restringida por las capacidades del hardware actual. Pero si el mensaje es extraído y almacenado, puede ser que con la llegada de nuevas tecnologías (como los computadores cuánticos o redes de computadores cuánticos) se tendrá suficiente potencia de computación para descifrar dichos mensajes. En cambio con la criptografía cuántica el descifrado de la clave cuántica no es posible. La idea central de la seguridad difiere en el hecho de que en criptografía clásica la seguridad del sistema se basa en la excesiva potencia de computación necesaria para romperlos, mientras en criptografía cuántica la seguridad del sistema se fundamenta en un principio básico de la mecánica cuántica que afirma que un qubit no puede ser medido sin perturbarlo-colapsarlo y por tanto corromper la clave. Otra diferencia entre la criptografía clásica y la criptografía cuántica es que en criptografía cuántica la transmisión de los qubits es continua, debido a que los qubits no se pueden copiar ni almacenar. En cambio en criptografía clásica, el mensaje cifrado no necesita ser continuo. Puede ser almacenado y transmitido en partes o en cualquier forma deseada, lo cual no se cumple en criptografía cuántica. Los repetidores cuánticos inventados durante los años noventa para almacenar los estados del fotón están siendo mejorados para conseguir un suficiente nivel de fiabilidad. No obstante no se han aplicado aún en la práctica y son un sujeto de especulación teórica.

Postulados de la mecánica cuántica. Evolución de un sistema cuántico.

Los principales postulados de la mecánica cuántica nos permiten conocer como representar los sistemas físicos, como representar las observaciones, como realizar las medidas y

como evolucionan los sistemas cuánticos cuando no se miden. Son los siguientes:

Postulado–1.

Cualquier sistema físico aislado/cerrado esta asociado con un espacio vectorial complejo donde se define un producto interno (espacio de Hilbert) que se denomina espacio de estado del sistema. El sistema se describe de forma completa por un vector de estado, un vector unitario del espacio de Hilbert. Este postulado proporciona el modelo matemático universal de cualquier sistema físico: un espacio vectorial de Hilbert sobre los números complejos, donde $i = (-1)^{1/2}$.

Los estados de los sistemas físicos se representan por medio de vectores en espacios vectoriales complejos denominados de Hilbert.

Postulado- 2.

La evolución de un sistema cuántico cerrado se describe por medio de una transformación unitaria. Esto es, el estado $|w(t)>$ del sistema en el instante de tiempo t esta relacionado con el estado $|w(t_0)>$ en el instante t_0 por medio de un operador unitario U que depende sólo de los instantes t y t_0.

Es decir: $|w(t)> = U \,.\, |w(t_0)>$. Este postulado describe la evolución temporal de un sistema físico cerrado.

❖ Fases del protocolo BB84 tipo *QKD* (*Quantum Key Distribution*) desarrollado por *C.H. Brassard* y *G. Bennett* en 1984:

- La entidad A transmite en forma de *qubits* una cadena binaria por ejemplo de 12 bits eligiendo sus bases cuánticas de forma aleatoria. La entidad B registra los resultados que recibe eligiendo de forma aleatoria sus bases cuánticas. Sobre una línea pública B informa a A de la elección de sus bases cuánticas.
- A compara con su elección de bases cuánticas y por una línea pública informa a B las medidas que eliminará, por ser incorrectas, por ejemplo 6.
- Sobre una línea pública B informa a la entidad A de un subconjunto del resultado, por ejemplo tres bits.
- Si A encuentra que la tasa de error es menor que el 25% A y B concluyen que la comunicación fue segura, es decir sin escucha clandestina E. Los restantes bits, es decir 3, forman la clave privada compartida final entre A y B.

❖ Ejemplo de cómo operan A y B:

Bits de A	1	0	0	1	1	1	0	0	1	0	0	1
Base cuántica de A	+	X	+	X	X	+	+	X	+	X	X	+
Ángulo de polarización	| 0	\ 135	– 90	/ 45	/ 45	| 0	– 90	\ 135	| 0	\ 135	\ 135	| 0
Base cuántica de B	X	X	+	+	X	+	X	+	+	X	+	X
Resultado de B	1	0	0	0	1	1	0	1	1	0	1	1
¿Mismas bases cuánticas?	no	si	si	no	si	si	no	no	si	si	no	no
Bits cribados		0	0		1	1			1	0		
Comprobación de datos		si	no		si	no			si	no		
Clave privada obtenida			0			1				0		

❖ ¿Por qué un 25% o más de error indica la presencia de un escucha clandestino E entre A y B?: La entidad E elige sus bases cuánticas de forma aleatoria, detecta cada fotón que envía A y envía una copia a B. La probabilidad de error será: $P_{error} = (P_{E-elige-una-base-cuántica-erronea}) \cdot (P_{B-obtiene-un-resultado-incorrecto}) = 50\% \cdot 50\% = 25\%$.

❖ Tres tipos de errores del sistema sin presencia de E: (1) *Borrado aleatorio de fotones* causados por absorción/dispersión o ineficiencia del detector, afecta a la eficiencia pero no a la seguridad. B dice a A las bases cuánticas usadas. (2) Si el medio en que viajan los fotones es birrefringente entonces el ángulo de polarización del fotón cambiará. (3) Cuentas incorrectas del detector de fotones, ocurre cuando los fotones que envía A no llegan a B y el detector de B registra un resultado debido a la fluctuación térmica.

Fig. 1.- Protocolo *BB84* tipo *QKD* con tecnología *SPS*.

Postulado–3.

Las medidas cuánticas se describen por medio de un conjunto $\{M_m\}$ de operadores de medida. Estos operadores actúan en el mismo espacio del sistema que se mide. El índice m se refiere a los resultados de medida que pueden ocurrir en el experimento.

Si el estado del sistema antes de la medida es $|w>$, la probabilidad de que el resultado m ocurra esta dado por la expresión:

$p(m) = <w|(M_m)^+ M_m|w>$;

donde M^+ es la adjunta de M.

El estado del sistema después de la medida es:

$(M_m|w> / (w|(M_m)^+ M_m|w>)^{1/2})$.

Los operadores de medida satisfacen la ecuación de completitud:

$$\sum_m (M_m)^+ M_m = I$$

Este postulado tiene que ver con las medidas cuánticas e indica la forma de extraer información de un sistema cuántico en un instante preciso de tiempo.

Las cantidades que pueden ser observadas o medidas se representan por medio de operadores hermíticos que actúan sobre los estados en espacios de Hilbert. Un operador o transformación M es hermítica si: $M^+ = M$, donde M^+ es la matriz adjunta de M. Una transformación es normal si: $M^+ . M = M . M^+$. Las transformaciones hermíticas son siempre normales.

Una transformación cuya inversa es su adjunta: $U^+ . U = I$ es una transformación unitaria. Las transformaciones unitarias son normales.

Una transformación cuyo cuadrado es igual a ella misma es decir: $M^2 = M$ se denomina proyector.

La Regla de Born afirma que cuando se realiza una medida, el estado del sistema físico se colapsa a uno de los valores propios o autovalores del operador hermítico que representan el observable. La probabilidad con que sucede esto está dada por el cuadrado del módulo del solapamiento entre los valores propios y el estado actual.

Dada la matriz:

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

los autovalores se obtienen de las raíces de la ecuación:

$$\det\begin{bmatrix}2-\lambda & 1\\ 1 & 2-\lambda\end{bmatrix} = (2-\lambda)^2 - 1 = 0$$

cuyo resultado es: $\lambda = 1$ y $\lambda = 3$. Los autovectores de la matriz A se obtienen para cada valor de λ; para $\lambda = 3$ se plantea la ecuación matricial:

$$\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} = 3\begin{bmatrix}x\\ y\end{bmatrix}$$

que conduce a x = y, si x = 1 entonces y $\lambda = 1$ y el autovector es:

$$\begin{bmatrix}1\\ 1\end{bmatrix}$$

para =1 se plantea la ecuación matricial :

$$\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}x\\ y\end{bmatrix}$$

que conduce a x = - y, si x = 1 entonces y = - 1 y el autovector es:

$$\begin{bmatrix}1\\ -1\end{bmatrix}$$

Dado el estado cuántico: $|w> = a.|0> + b.|1>$, superposición coherente de los estados de base: $|0>$ y $|1>$, se puede medir $|w>$ utilizando una POVM (Positive Operator Valued Measurement) que define una familia de operadores hermíticos, un caso simple son los proyectores ortogonales: $|M><M|$. Esta medida de proyección simple se denomina medida von Neumann. El resultado de una medida von Neumann ocurrirá con probabilidad $|<w|M>|^2$. Si un qubit representa el estado de polarización de un fotón, donde la polarización horizontal se denota por $|0>$ y la polarización vertical se representa por $|1>$, estos dos estados son ortogonales ya que: $<0|1> = 0$.

- El protocolo BB84 del tipo *QBC* (*Quantum Bit Commitment*) es un protocolo *BC* basado en la física cuántica, es debido a *C.H. Brassard* y *G. Bennett*. No es incondicionalmente seguro, en cambio el protocolo BB84 del tipo *QKD* si.
- FASES DEL PROTOCOLO *QBC*: (1) *Fase de compromiso de A con B*. A elige un bit b y s bits aleatorios $\{b_i\}$. La entidad A envía a la entidad B s qubits en forma de fotones, cada uno codificando b_i con respecto a la base $\{-, |\}$ si $b = 0$ o a la base $\{/, \backslash\}$ si $b = 1$. La entidad B elige s bits aleatorios $\{b'_i\}$ y mide los qubits recibidos con respecto a la base cuántica $\{-, |\}$ cuando $b'_i = 0$ o a la base $\{/, \backslash\}$ cuando $b'_i = 1$. (2) *Fase de revelación de A a B*: A revela a la entidad B los valores: b y $\{b_i\}$. La entidad B verifica que b fue medido para todos los i tales que $b_i = b'_i$.
- Las probabilidades de medir 0 o 1 dependen de los valores de b, b_i y b'_i es:

b	b_i	Qubit enviado	b'_i	Base de medida	Probabilidad de medir 0	Probabilidad de medir 1
0	0	–	0	{–, |}	1	0
0	0	–	1	{/, \}	½	½
0	1	|	0	{–, |}	0	1
0	1	|	1	{/, \}	½	½
1	0	/	0	{–, |}	½	½
1	0	/	1	{/, \}	1	0
1	1	\	0	{–, |}	½	½
1	1	\	1	{/, \}	0	1

- Aquí b se oculta en la base cuántica, bien horizontal o rotada 45°. La entidad A envía una mezcla de estados ortogonales para confundir a B que no puede decir si recibe mezclados: – y | o mezclados / y \. Cuando A revela la lista de $\{b_i\}$, la entidad B puede confirmar que de hecho todas sus medidas dieron el correcto valor durante aproximadamente s/2 veces que b_i era igual a b'_i.

Fig. 2.- Protocolo *BB84* tipo *QBC*.

Postulado–4.

El espacio de estado de un sistema físico compuesto, es el producto tensorial de los espacios de estado de los sistemas físicos componentes. Así mismo, si tenemos un sistema cuántico H_i con i = 1, 2, …, n y el sistema H_i esta preparado en el estado $|w_i>$, entonces el estado conjunto del sistema total es: $|w_1>\otimes|w_2>\otimes...\otimes|w_n> = H_1\otimes...\otimes H_n$. Este postulado formaliza la interacción de muchos sistemas físicos con la combinación de diferentes espacios de Hilbert en un único espacio de Hilbert. Se cumple que:

$|x>\otimes|y> = |x>|y> = |xy>$

Postulado–5.

Sea $|w(t)>$ el estado de un sistema mecánico cuántico cerrado S (por ejemplo de un fotón) como una función del tiempo t. Entonces el comportamiento dinámico del sistema S viene determinado por la ecuación de Schrödinger:

$$\frac{\partial}{\partial t}|w(t)> = -\left(\frac{i}{h}\right)H|w(t)>$$

donde h es la constante de Planck y H representa un observable de S denominado Hamiltoniano. El Hamiltoniano es el análogo en mecánica cuántica del Hamiltoniano de mecánica clásica. En mecánica clásica H representa la energía total del sistema. La ecuación de Schrödinger describe la evolución de un sistema cuántico (por ejemplo un fotón) cuando no se hacen medidas.

Qubit. QKD. Polarización de fotones. Tipos de transmisión.

Un qubit es el sistema mecánico cuántico más simple, un espacio de estado de dos dimensiones y permite transportar los bits de información 0 y 1. Supongamos que $|0>$ y $|1>$ forman una base ortonormal para el espacio de estado, entonces un vector de estado arbitrario en el espacio de estado puede escribirse como $|w> = a.|0> + b.|1>$ donde a y b son números complejos. Utilizando la notación BRAKET de P.A.M. Dirac:

$|w> = \begin{bmatrix}a\\ b\end{bmatrix}$ es un ket y $<w| = (a', b')$ es un bra, donde a' es el conjugado complejo de a.

El producto interno entre el vector ket $|w>$ y el vector ket $|q>$ es $<w|q>$. Con un qubit sólo tenemos una superposición de dos estados: $|0>$ y $|1>$. Con dos qubits tenemos una superposición de cuatro estados: $|00>$, $|01>$, $|10>$, $|11>$. Se cumplen algunas propiedades:

Principio de superposición.

Un fotón puede estar en dos estados simultáneamente de forma coherente, por ejemplo polarizado horizontal y verticalmente.
Es decir: $|w>= a.|0>+ b.|1>= \begin{bmatrix} a \\ b \end{bmatrix}$
donde: $|0>=\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1>=\begin{bmatrix} 0 \\ 1 \end{bmatrix}$;
$|a|^2+|b|^2= 1$, siendo a y b números complejos; se medirá el estado $|0>$ con probabilidad $|a^2$ y se medirá el estado $|1>$ con probabilidad $|b|^2$.

Interferencia.

Un fotón en superposición puede interferir consigo mismo. Un fotón puede viajar por dos caminos a la vez existiendo superposición que da lugar a la interferencia.

Medida cuántica.

Dado el qubit: $|w>=a.|0>+b.|1>$, el proceso de medida es la proyección sobre el eje $|0>$ o sobre el eje $|1>$, de modo que se observa 0 con una probabilidad $|a|^2$ y se observa 1 con una probabilidad $|b|^2$. Después de la medida el qubit estará en $|0>$ o $|1>$. Por tanto, la medida cambia el estado es decir se produce "collapsed it".

- Un *qubit* o *bit cuántico* es un objeto cuántico elemental utilizado para almacenar y transmitir información.
- El *estado de un qubit* $|w>$ es un vector en un espacio vectorial complejo de dos dimensiones. En este espacio, un vector tiene dos componentes y las proyecciones del vector en una base del espacio vectorial son números complejos.
- La *notación de Dirac* permite representar un vector *ket* como: $|w> = a_0|0> + a_1|0> = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$, donde a_0 y a_1 son números complejos y los kets $|0> = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ y $|1> = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ los vectores que forman una *base ortonormal* para este espacio vectorial de dos dimensiones.
- El estado de un qubit puede representarse por: $|w> = a_0|0> + a_1|0>$ donde $|0>$ y $|1>$ es un par de vectores de base ortonormales denominados *estados de base*. La única restricción en los coeficientes es que: $|a_0|^2 + |a_1|^2 = 1$; tal estado se denomina *superposición de los vectores de base*.
- Cuando *medimos u observamos* el estado $|w>$ de un qubit se obtiene el resultado: $|0>$ con *probabilidad* $|a_0|^2$ y $|1>$ con probabilidad $|a_1|^2$ donde $|a_0|^2 + |a_1|^2 = a'_0.a_0 + a'_1a_1 = 1$ donde a'_1 con i = 0,1 es el *conjugado complejo* de a_1. Si $x = 2 + 3i \rightarrow x' = 2 - 3i$ con $i = \sqrt{-1}$.
- El *qubit*: $\frac{1}{2}|0> + \frac{\sqrt{3}}{2}|1>$ está en un *estado de superposición* hasta que lo medimos y el qubit conduce al resultado $|0>$ con probabilidad ¼ y al resultado $|1>$ con probabilidad ¾.
- La superposición y el efecto de la medida de un estado cuántico (*estado del qubit*) significa que existe información oculta que se preserva en un *sistema cuántico cerrado* hasta que es forzado a revelarlo a un observador externo. Se dice que el sistema esta cerrado hasta que interactúa con el mundo exterior, por ejemplo, hasta que realicemos una *observación del sistema*.
- Un sistema físico cuántico que conduce a la encarnación más simple posible de un qubit es el *fotón* que presenta dos polarizaciones independientes, por ejemplo: horizontal (–) y vertical (|), de forma conjunta *polarización lineal* (+) y a la derecha (/ = +45°) y a la izquierda (\ = - 45°) de forma conjunta (X) en el caso de *polarización diagonal o circular*.

Fig. 3.- Relación entre qubits y fotones polarizados.

No clonación.

Un hipotético escucha clandestino E situado entre A y B no puede copiar el qubit enviado por A. Este principio es la base de la seguridad de los protocolos QKD (Quantum Key Distribution).

Indistinguibilidad de estados no ortogonales.

Estados entanglement.

La medida de parte del sistema colapsa a un estado que es consistente con el resultado de la medida. Un estado EPR o estado Bell se puede representar como:

$|w^+> = 2^{-1/2}(|00> + |11>)$.

Si se mide la primera parte, la segunda parte estará completamente correlacionada incluso si ambas partes se encuentran separadas:
$|w^+> = 2^{-1/2}(|00> + |11>)$ con probabilidad ½ se obtiene $|00>$ o $|11>$. No sabiendo el resultado de la medida, el segundo qubit tiene una distribución de probabilidad sobre $|0>$ y $|1>$. En el estado entangled (estado Bell):

$$|w^+> = \frac{1}{\sqrt{2}}(|00> + |11>)$$

la entidad A tiene el primer fotón y B el segundo. Una propiedad de este estado es que tiene la misma forma en base rectilínea + y en base diagonal X ya que:

$$|w^+> = \frac{1}{\sqrt{2}}(|0>_+|0>_+ + |1>_+|1>_+) = \frac{1}{\sqrt{2}}(|0>_X|0>_X + |1>_X|1>_X).$$

Esto significa que los resultados de las medidas de A y B están completamente correlacionados cuando miden el estado $|w^+>$ en cualquiera de las bases. Si A y B generan una clave preparan un gran número de estos estados Bell:

$$|w^+>^{\otimes n} = |w^+> \otimes \ldots \otimes |w^+>.$$

Un sistema de distribución cuántica de clave secreta o QKD es un sistema de telecomunicaciones que puede crear una clave simétrica perfectamente segura en el transmisor y en receptor. Necesita dos canales de comunicaciones:
(a) Un canal cuántico, donde se transmiten los bits cuánticos o qubits en forma de fotones.
(b) Un canal público clásico, para las

comunicaciones de mensajes clásicos entre el transmisor y el receptor. Se ha demostrado que QKD posee la propiedad de la seguridad incondicional. De modo que es seguro contra cualquier tipo de ataque incluso si el atacante posee potencia de computación infinita e infinita cantidad de dinero.

La polarización es una propiedad intrínseca de un fotón. Los fotones pueden estar polarizados horizontalmente, verticalmente diagonalmente con 45º y diagonalmente con 135º. Sólo se puede medir polarización con respecto a alguna dirección especificada. En cualquier medida sólo podemos obtener uno de los dos siguientes resultados 0 o 1. Si la entidad A envía a la entidad B la secuencia de bits 1011101 con la base VDDDVVD (donde V es vertical y D diagonal) y B aplica la base VVDVDVD entonces los bits recibidos correctos serán 1*1***01.

Bases cuánticas. Codificación de bits en Qubits. Tipos de errores en un Qubit.

Uno de los propósitos de la criptografía cuántica es proporcionar una forma segura para intercambiar una clave secreta (también denominada clave simétrica o secreto compartido). Existen dos esquemas básicos de funcionamiento, el primero se basa en el uso de una única partícula o fotón es el más implementado, utiliza la tecnología SPS (Single-Photon-Source) y el otro utiliza estados cuánticos entangled (estados no separables, es decir estados que presentan una fuerte correlación entre sí). Los protocolos cuánticos pueden utilizar cualquier par de polarización ortogonal, por ejemplo: En la base cuántica + el bit 1 se representa, cuantifica y codifica como | | > (corresponde a 0º) y el bit 0 se cuantifica/codifica como | – > (corresponde a 90º); en la base cuántica X el bit 1 se representa como | / > (corresponde a 45º) y el bit 0 como | \ > (corresponde a 135º). Un dispositivo electrónico denominado PC (Pocket Cell) se encarga de rotar la polarización (o vector de polarización) de cada fotón procedente de una fuente de único fotón los ángulos de 0º, 45º, 90º y 135º. La criptografía cuántica puede utilizar fibra óptica como medio de transmisión o bien el espacio libre donde los fotones viajan por el aire, en este caso se utilizan telescopios para dirigir y recoger los fotones; en criptografía cuántica por espacio libre el emisor dispone de una SPS seguido de un telescopio y el receptor posee otro telescopio seguido de un detector de polarización y fotones. Los dispositivos denominados PBS (Polarizer Beam Splitter) discriminan la polarización de los fotones recibidos si es vertical, horizontal, etc. Actualmente se consiguen en criptografía cuántica por espacio libre distancias de 144 Km y el objetivo es desarrollar sistemas que se comuniquen vía satélite.

Los principales tipos de errores en un qubit son:

1) Errores de cambio de estado.

Cuando el estado |0> se convierte en |1> y viceversa. El error se describe por la matriz de Pauli :

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

2) Errores de fase.

Transforman el estado |1> en – |1>, pero deja al estado |0> sin cambios. Tal error se describe por la matriz de Pauli:

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

3) Errores combinados.

Cuando se cambia el |0> a – |1> y |1> a |0>. Se describe por la matriz de Pauli:

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \sigma_z \sigma_x$$

- Si dos entidades separadas A y B poseen *qubits* en forma de fotones separados a y b que se encuentran en estado fuertemente correlacionado (*estado entangled*) entonces A puede obtener información sobre la medida de b por parte de la entidad B midiendo a. Dicho de otro modo más técnicamente, el espacio de estado cuántico de un conjunto de fotones es el producto directo de sus espacios individuales.
- Utilizando esta paradoja la entidad A puede hacer trampas en el protocolo BB84 tipo *QBC*. Las *fases del protocolo* son: (1) *Fase de compromiso de A a B*: La entidad A fabrica s pares de *qubits entangled*: $1/\sqrt{2}$ |– –> + $1/\sqrt{2}$ | | | > y envía un qubit/fotón del par mientras guarda el otro. (2) *Fase de revelación del compromiso asumido por A a B*: La entidad A mide sus propios qubits con respecto a la base rectilínea { – , | } si desea revelar un valor 0 y con respecto a una base diagonal { / , \ } si desea revelar un valor 1. La entidad A envía el bit revelado junto con los resultados de sus medidas b''_i. Una medida colapsa o perturba el estado cuántico del qubit/fotón en el subespacio que es compatible con el valor obtenido. La entidad A explota el hecho de que el estado: $1/\sqrt{2}$ |– –> + $1/\sqrt{2}$ | | | > = $1/\sqrt{2}$ | / / > + $1/\sqrt{2}$ | \ \ > esta totalmente correlacionado o *entangled* con respecto a ambas bases cuánticas. Cuando A mide su qubit con respecto a la base horizontal obtiene bien 0 o 1 con probabilidad del 50%. Sin embargo esto proyecta el espacio de estados entero del *par entangled* a |– –> o | | | > ya que las componentes |– |> y | |–> son cero desde el principio, lo cual significa que B obtendrá el mismo resultado (*paradoja de ERP, Einstein-Podolsky-Rosen*).
- La entidad A puede hacer trampas en el protocolo BB84 del tipo QBC:

Par qubit	Base cuántica de A	b''_i	Nuevo estado	b'_i	Base cuántica de B	Probabilidad de 0	Probabilidad de 1
$1/\sqrt{2}$ |– –>	{ – , | }	0	| – – >	0	{ – , | }	1	0
+				1	{ / , \ }	½	½
$1/\sqrt{2}$ | | | >	{ – , | }	1	| | | >	0	{ – , | }	0	1
=				1	{ / , \ }	½	½
$1/\sqrt{2}$ | / / >	{ / , \ }	0	| / / >	0	{ – , | }	½	½
+				1	{ / , \ }	1	0
$1/\sqrt{2}$ | \ \ >	{ / , \ }	1	| \ \ >	0	{ – , | }	½	½
=				1	{ / , \ }	0	1

- Con este procedimiento A asegura que si $b''_i = b_i$, B utiliza la misma base para realizar su medida, de modo que obtendrá un resultado idéntico. Cuando el ángulo entre el estado y la base es 45º, B obtiene una distribución 50%-50% como se esperaba.

Fig. 4.- Paradoja EPR y su aplicación para que A haga trampas en el protocolo BB84 tipo *QBC*.

Estrategias de escucha clandestina en criptografía cuántica.

Las principales estrategias de escucha clandestina son:

(1) La escucha clandestina opaca (tipo activo).

El atacante E intercepta el mensaje enviado por la entidad A y a continuación suplanta a la entidad A frente a la entidad B enviándole a B el mensaje recibido de A con destino a B. Este tipo de ataque también se denomina MITM (Man-In-The-Middle). En este tipo de ataque un escucha clandestino E se supone que tiene la capacidad de monitorizar el canal de comunicaciones e insertar y eliminar mensajes con precisión y sin retardo. Cuando la entidad origen A intenta establecer una clave secreta con una entidad remota B, la entidad E intercepta y responde a los mensajes en ambas direcciones, haciendo creer a A y a B que se comunican con B y A respectivamente. Una vez establecida la clave E recibe, copia y reenvía mensajes permitiendo que A y B se comuniquen. Asumiendo que el tiempo de procesamiento y la precisión no son dificultades, la entidad E puede recuperar la clave secreta y de este modo el texto sin cifrar de cada mensaje enviado entre A y B sin dar signos detectables de la presencia de E. Debido a la dificultad de utilizar únicos fotones para la transmisión, muchos sistemas emplean pequeñas ráfagas de luz láser. En teoría la entidad E puede dividir fotones individuales de la ráfaga reduciendo su intensidad pero no afectando su contenido. Observando estos fotones (si es necesario guardarlos hasta que sea anunciada la base correcta para observación) E puede obtener información sobre la información transmitida de la entidad A a la entidad B.

- Los fotones no tienen masa, se caracterizan por su momento vector que determina su *frecuencia* y su *polarización*. Un fotón es un TSQS (*Two-State Quantum System*) muy importante utilizado para transportar un *qubit*.
- Un fotón puede tener dos polarizaciones independientes y los sistemas que utilizan la polarización de un fotón para codificar información binaria se utilizan en criptografía cuántica.
- Desde el punto de vista de polarización, un fotón puede describirse como un TSS (*Two-State System*). Un fotón puede estar en el estado $|h\rangle$ o en el estado $|v\rangle$. Todos los fotones en un haz de luz polarizado en el eje horizontal se dice que están en el estado de polarización $|h\rangle$ y similarmente todos los fotones en un haz de luz polarizado en un eje vertical se dice que están en el estado de polarización $|v\rangle$. Los estados $|h\rangle$ y $|v\rangle$ pueden utilizarse como *estados base* para describir la polarización de un fotón de un haz de luz polarizado rectilineamente.
- Un *qubit en general* se describe como el vector ket: $|w\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = a.|0\rangle + b.|1\rangle$ con la base canónica en C^2: $\{ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ cuantifica el 0, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ cuantifica el 1$\}$ o como el bra: $\langle w| = (a', b') = a'.\langle 0| + b'.\langle 1|$ donde $\langle 0| = (1\ 0)$ y $\langle 1| = (0, 1)$, utilizando la notación de Dirac.
- El *producto interno*: $\langle w_1|w_2\rangle = \langle w_1, w_2\rangle = a'_1.a_2 + b'_1.b_2$. Así mismo: $\langle i|j\rangle = \delta_{ij}$ ($\delta_{ij} = 1$ si $i = j$, $\delta_{ij} = 0$ si $i \neq j$).
- El producto externo es un operador: $|w_1\rangle\langle w_2| = \begin{bmatrix} a_1.a'_2 & a_1.b'_2 \\ b_1.a'_2 & b_1.b'_2 \end{bmatrix}$ donde *traza* (suma elementos diagonal principal): $Tr(|w_1\rangle\langle w_2|) = \langle w_2|w_1\rangle$. Así mismo $\langle w|w\rangle = |a|^2 + |b|^2 = 1$. La *interpretación de Born* de un *qubit* es: $|a|^2 = Prob(x = 0) = |\langle w|0\rangle|^2$ y $|b|^2 = Prob(x = 1) = |\langle w|1\rangle|^2$. La *proyección sobre w* $= |w\rangle\langle w|$. Si $p_i \geq 0$ con $\sum_i p_i = 1$, las *matrices densidad* (mezclas estadísticas de estados) son: $\rho = \sum_i p_i |w_i\rangle\langle w_i|$ donde $\rho \geq 0$ y traza $Tr(\rho) = 1$. Evolución de los qubit con las *matrices de Pauli* (son operadores unitarios): $X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$; $Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i.X.Z$; $Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$; $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \sum_{i=0}^{N-1} |i\rangle\langle i|$. El *conmutador de dos matrices A y B* es: [A, B] = A.B – B.A. El *anticonmutador de dos matrices A y B* es: {A, B} = A.B + B.A. Para las matrices de Pauli: [-Y, X] = [X, Y] = i.Z; [-Z, Y] = [Y, Z] = i.X; [Z, X] = - [X, Z] = i.Y; {X, Y} = {Y, Z} = {Z, X} = 0.

Fig. 5.- Aspectos matemáticos en *QC*.

(2) La escucha clandestina traslúcida o convencional (tipo pasivo).

A su vez pueden ser de dos tipos:

(a) Escucha traslúcida sin entanglement. El adversario o entidad E hace que la portadora de información interactúe unitariamente con su sonda y a continuación deja que siga hasta B en un estado ligeramente modificado: $\{|0\rangle|w\rangle$ pasa a: $|0'\rangle|w_+\rangle$; $|1\rangle|w\rangle$ pasa a: $|1'\rangle|w_-\rangle\}$ donde $|w\rangle$ representa el estado de la sonda.

(b) Escucha traslúcida con entanglement. Para aumentar su información la entidad E puede intentar entangle el estado de su sonda y la portadora que reenvía:

$|0\rangle|w\rangle$ pasa a:
$a|0'\rangle|w_+\rangle + b|1'\rangle|w_-\rangle$;
$|1\rangle|w\rangle$ pasa a:
$b|1'\rangle|w_-\rangle + a|0'\rangle|w_+\rangle$.

Un factor que confunde a la hora de detectar ataques es la presencia de ruido en el canal de comunicaciones cuántico. La escucha clandestina y el ruido son indistinguibles para las partes A y B que se comunican de modo que pueden causar que falle el intercambio cuántico seguro. Esto conduce a un problema potencial: un escucha clandestino malicioso puede impedir que ocurra la comunicación (ataque de Denegación de Servicios o DoS) escuchando de forma continuada, lo cual genera ruido y no habrá acuerdo de clave QKD.

Tipos de ataques a protocolos QKD. Estados cuánticos puros y entanglement de estados puros.

Los principales ataques a criptosistemas cuánticos pueden clasificarse en dos categorías: los ataques dirigidos al propio protocolo como el ataque MITM (Man-in-the-Middle) o BB (Bucket-Brigade). Aquí el atacante E realiza conexiones independientes con A y B y retransmite los mensajes entre ellos haciendo creer que se comunican directamente entre si mientras que la comunicación la controla E. La entidad E debe poder interceptar todos los mensajes que circulan entre A y B y reenviar los nuevos lo cual es posible en la mayoría de las circunstancias. El ataque MITM opera mejor cuando E puede suplantar cada punto final a la satisfacción del otro. La mayoría de los protocolos criptográficos incluyen alguna forma de autenticación del punto final para prevenir el ataque MITM. Por otra parte, los ataques dirigidos hacia la implementación del protocolo como:

(1) Ataque PNS (Photon Number Splitting).
(2) Ataque BS (Beam-Splitting).
(3) Ataque RNG (Random Number Generador).
(4) Ataque SC (Side-Channel).

Si el estado:

$$|w12> \neq |w1> \otimes |w2>$$

entonces el estado $|w>$ es entangled. Un sistema cuántico compuesto consta de un conjunto de subsistemas cuánticos, se describe matemáticamente como:

$$|w> = \frac{1}{\sqrt{2}}(|0>|1> + |1>|0>)$$

donde el primer ket en cada producto pertenece a un fotón y el segundo al otro. Consideremos un estado del tipo GHZ (Greenberger-Horne-Zeilinger):

$$\frac{1}{\sqrt{2}}(0>|0>|0> + |1>|1>|1>),$$

se cumple que la observación del estado de uno de los subsistemas instantáneamente permite conocer el estado de los otros dos.

- La entidad A elige de forma aleatoria 2n *qubits*, cada uno, en uno de los cuatro posibles *estados*: $\{|0>_+, |0>_\times = H.|0>_+, |1>_+, |1>_\times = H.|1>_+$, donde la *transformación* unitaria *de Hadamard* es: $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ con $H^2 = 1\}$ y los envía a la entidad B a través de un *canal cuántico de comunicaciones*. Por cada qubit que recibe B, éste elige de forma aleatoria una de las dos *bases cuánticas* + (rectilínea) o X (diagonal) y mide el qubit con respecto a ella. En el caso de un canal sin ruido, si B elige la misma base que A, el resultado de su medida es el mismo, si las bases difieren el resultado de B será aleatorio. A informa a B utilizando un *canal clásico de comunicaciones* que base utilizó para cada qubit. A y B mantienen los bits donde se utilizó la misma base para su medida. Esto sucede aproximadamente en la mitad de los casos, de modo que dispondrán aproximadamente de n bits comunes (denominados *clave cribada*). A y B eligen un subconjunto de la clave cribada para estimar la tasa de error. A y B se anuncian públicamente los valores de los bits de dicho subconjunto. Si difieren en demasiados casos abortan el protocolo ya que su seguridad no puede garantizarse (existencia de un escucha clandestina E). Finalmente A y B obtendrán *una clave secreta conjunta* a partir de los bits restantes realizando *corrección de errores* (A elige dos bits aleatorios y dice a B el valor XOR, B dice a A si tiene el mismo valor, en este caso guardan el primer bit y descartan el segundo, si los valores difieren descartan ambos bits) y *amplificación de privacidad* (consiste en que A y B eligen de forma aleatoria pares de bits de la clave cribada y los sustituyen por sus valores XOR, de esta forma se divide entre dos la longitud de la clave).
- *CASO 1*:

2n bits enviados por A (14 bits)	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Base de A	+	+	+	X	X	+	X	X	X	X	+	+	+	+
Base de B	+	X	+	+	X	+	X	+	X	X	+	+	+	+
Bits recibidos por B	1	?	0	?	0	0	1	?	1	1	1	1	0	0
¿Misma base?	SI	NO	SI	NO	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
Bits a guardar (clave cribada)	1		0		0	0	1		1	1	1	1	0	0
Comprobación	SI		NO		NO	SI	NO		NO	NO	NO	SI	SI	NO
Clave secreta final compartida			0		0		1		1	1	1			0

? => Bit aleatorio.

- *CASO 2*:

Base de A	+	X	X	+	+	X	+
Qubit envía A	–	\	/	|	|	/	–
Base de B	+	+	X	+	X	X	+
Medida de B	–	|	/	|	\	/	–
Bits compartidos	0		0	1		0	0

Fig. 6.- Dos casos de acuerdo de clave secreta tipo *QKD BB84*.

Criptosistema simétrico QOTP.

Un criptosistema QOTP (Quantum One-Time-Pad). se utiliza para cifrar de forma simétrica un cierto texto en claro. Presenta cierta similitud con el criptosistema OTP (One-Time-Pad) clásico en el que se desea cifrar un cierto texto en claro p formado por una cadena de n bits, existe una clave secreta k compartida entre los extremos de la comunicación de n bits de longitud y el texto cifrado c de n bits de longitud se obtiene a través de la operación o-exclusiva:

$$c = (p + k) \bmod 2.$$

Para descifrar se utiliza la expresión:

$$p = (c + k) \bmod 2.$$

El criptosistema QOTP utiliza como texto en claro una cadena de n qubits: $|p> = |p_1> \ldots |p_n>$. Emplea como clave secreta compartida dos cadenas de n bits cada una: k, k'. El texto cifrado es una cadena de n qubits: $|c> = |c_1> \ldots |c_n>$. El proceso de cifrado se realiza a través de la expresión:

$$|c_i> = (\sigma_x)^{k_i} (\sigma_z)^{k'_i} |p_i>$$

El proceso de descifrado se realiza a través de la expresión:

$$|p_i> = (\sigma_z)^{k'_i} (\sigma_x)^{k_i} |c_i>$$

donde los qubits:

$$|p_i> = \begin{bmatrix}a_i\\ b_i\end{bmatrix} \text{ y } |c_i> = \begin{bmatrix}d_i\\ e_i\end{bmatrix};$$

además: (σ_x, σ_z) son matrices de Pauli. La razón por la cual el criptosistema QOTP es absolutamente seguro

es la siguiente: En un criptosistema QOTP un qubit w se transmite utilizando un estado mezclado:

$\{(1/4, |w\rangle), (1/4, \sigma_x|w\rangle), (1/4, \sigma_z|w\rangle), (1/4, |\sigma_x \sigma_z w\rangle)\}$

cuya matriz de densidad es:

$(\frac{1}{2}\ I_2)$ que es la misma que la matriz de densidad para el estado mezclado $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ que corresponde a la transmisión de un bit aleatorio.

Protocolo criptográfico cuántico de tres etapas de KAK.

El protocolo criptográfico cuántico de tres etapas debido a Kak es un protocolo puramente cuántico ya que la información intercambiada entre A y B se efectúa utilizando únicamente un canal cuántico. En cambio el protocolo QKD BB84 es híbrido ya que utiliza dos canales, uno cuántico y otro convencional.

Dadas dos transformaciones U_A y U_B que conmutan, la secuencia de etapas del protocolo criptográfico cuántico de tres etapas de Kak es la siguiente:

(1) A aplica la transformación U_A sobre el qubit secreto S y se lo envía a B.

(2) B aplica la transformación U_B al qubit recibido $U_A(S)$ y lo reenvía a A.

(3) A aplica la transformación inversa $(U_A)^{-1}$ al qubit recibido convirtiéndolo en U_B (S) y lo reenvía a B.

(4) B aplica la transformación inversa $(U_B)^{-1}$ al qubit convirtiéndolo en S. Las entidades A y B deben acordar utilizar operadores de transformación de un conjunto mutuamente decidido, pueden ser operadores de Pauli y otros más complejos. A y B pueden trabajar con dos qubits en este caso las transformaciones que pueden utilizar son matrices de 4x4 como:

$$U_A = U_B = 1/2 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix};$$

$$U_A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \text{ o bien } \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

$$U_B = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \text{ o bien } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

No es conveniente utilizar operadores de rotación.

- Dado el estado cuántico expresado como expansión de estados de base: $|w\rangle = \sum_{x\in\{0,1\}} a_x |x\rangle$ la probabilidad de medir x es: $Pr(x) = |a_x|^2 = |\langle x|w\rangle|^2$
- El producto tensorial: $A \otimes B = \begin{bmatrix} a_{11}.B & a_{12}.B \\ a_{21}.B & a_{22}.B \end{bmatrix}$ donde $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ y $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ donde: dim (A ⊗ B) = dim(A) . dim(B). Un sistema de dos qubits: $|x\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ donde los estados base {|00>, |01>, 10>, |11>} son estados producto tensorial, por ejemplo: $|10\rangle = |1\rangle \otimes |0\rangle$. Otro estado producto tensorial es: $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$. Un estado Bell/ERP (*estado entangled*) es: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- *Distribución de clave sin escucha clandestina con una elección de asignación*:

Bits enviados por A (9 bits)	1	0	1	0	1	0	1	0	0
Qubits enviados por A	|	–	/	\	/	\	/	\	–
Base aleatoria de A	+	+	X	X	X	X	X	X	+
Base aleatoria de B	+	+	+	+	X	X	+	+	+
Bits medidos por B	1	0	0	0	1	0	1	1	0
¿Misma base?	SI	SI	NO	NO	SI	SI	NO	NO	SI
Clave cribada (clave secreta final compartida entre A y B)	1	0			1	0			0

- *Distribución de clave sin escucha clandestina con otra elección de asignación*:

Base aleatoria de A	+	X	X	+	+	X	+	X	+	X
Qubit envía A	| = 0	\ = 1	/ = 0	|	– = 1	/	–	\	|	/
Base aleatoria de B	+	X	+	X	+	+	X	X	+	+
Medida de B y bits compartidos	0	1	1	0	1	1	1	1	0	0

Fig. 7.- Bases de medida y distribución cuántica de claves.

Consideraciones finales.

Nuestro grupo de investigación lleva hace diez años trabajando en criptografía cuántica tanto para el desarrollo de comunicaciones protegidas cuánticas como para evaluar y reforzar diferentes criptosistemas cuánticos en presencia de ruidos y con atacantes. Se han utilizado como medios de transmisión fibra óptica y transmisiones inalámbricas con resultados muy satisfactorios y en algunos casos excelentes. Los principales desafíos en éste fascinante área de la criptografía son el desarrollo de protocolos cuánticos para firma digital, los servicios de autenticación, los mecanismos para preservar la privacidad y los que permiten las tareas de anonimato y ocultación de información como DWM cuánticas y esteganografía cuántica.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto LEFIS-APTICE (financiado por Socrates 2005-2007. European Commission).

Bibliografia

- Areitio, J. y Areitio, A. "Tipificación de amenazas, identificación de contramedidas de seguridad en el ámbito de gestión de redes y sistemas". Revista Española de Electrónica. Nº 613. Diciembre 2005.

- Areitio, J. "Diseño, síntesis y monitorización de criptosistemas simétricos". Revista Española de Electrónica. Nº 595. Junio 2004.

- Areitio, J. "Seguridad de la Información: Redes, Informática y Sistemas de Información". Cengage Learning Paraninfo. 2008.

- Dube, R.R. "Hardware-based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography". Wiley. 2008.

- Mollin, R. "An Introduction to Cryptography" CRC / Chapman and Hall. 2006.

- Busch, P., Lahti, P.J. and Mittelstaedt, P. "The Quantum Theory of Measurement". Springer-Verlag. New York. 1991.

- Dirac, P.A.M. "The Principles of Quantum Mechanics". Oxford University Press. Oxford. 1958.

- Peres, A. "Quantum Theory: Concepts and Methods". Kluwer Academic Publishers. Boston. 1993.

- Sakurai, J.J. "Modern Quantum Mechanics". Addison-Wesley Publishing Company. Reading Massachusetts. 1994.

- Morsch, O. "Quantum Bits and Quantum Secrets: How Quantum Physics is revolutionizing Codes and Computers". Wiley-VCH. 2008.

- Feynman, R.P., Leighton, R.B. and Sands, M. "The Feynman Lectures on Physics: Vol. III. Quantum Mechanics". Addison- Wesley Publishing Company. Reading. Massachusetts. 1965.

- Omnes, R. "An Interpretation of Quantum Mechanics". Princeton University Press. New Jersey. 1994.

- Penrose, R. "The Large, the Small and the Human Mind". Cambridge University Press. 1997.

- Marinescu, D.C and Marinescu, G.M. "Approaching Quantum Computing". Prentice-Hall, USR. NJ. 2004.

- Brown, J. "The Quest for the Quantum Computer". Simon and Schuster. New York. 1999.

- Feynman, R.P. "Lectures on Computation". Addison-Wesley. Reading. MA. 1996.

- Bell, J.S. "Speakable and Unspeakable in Quantum Mechanics". Cambridge University Press. 1987.

- Neumann, J. von "Mathematical Foundation of Quantum Mechanics". Princeton University Press. 1955.

- Barbieri, C., Cariolaro, G., Occhipinti, T., Pernechele, C., Tamburini, F. and Villoresi, P. "Qspace Project: Quantum Cryptography in Space Optical Communication Theory and Techniques". Springer. 2004.