Algoritmos cuánticos en criptografía y distribución de claves en espacio libre

Raúl Pérula Martínez
Profesor tutor: Pedro Antonio Gutiérrez Peña

ra_ules@informaticos.com

Resumen
En este artículo se ha realizado una breve introducción a la criptografía cuántica, en el cual se han visto los principales y más conocidos algoritmos en criptografía cuántica, BB84 y B92, junto con una mejora de uno de ellos, el K05. También se incluye información sobre un estudio experimental de uno de los temas más estudiados e interesantes, la distribución de claves cuánticas en el espacio libre (QKD).

Palabras Clave: criptografía cuántica, computación cuántica, algoritmo, distribución claves, QKD.

Abstract
This article has a brief introduction to quantum cryptography, which have been the largest and most well-known algorithms in quantum cryptography, BB84 and B92, along an improved one, K05. Also included information on an experimental study of one of the most studied and interesting topics, the quantum key distribution in free space (QKD).

Keywords: quantum criptography, quantum computing, algorithm, key distribution, QKD.

1. Introducción

1.1. Criptografía cuántica

La criptografía cuántica es una nueva área dentro de la criptografía que hace uso de los principios de la física cuántica para transmitir información de forma tal que solo pueda ser accedida por el destinatario previsto.

La criptografía cuántica hace uso de dos canales de comunicación entre los dos participantes. Un **canal cuántico**, el cual tiene un único sentido y que generalmente es de fibra óptica. El otro canal es un **canal convencional, público y de dos vías**, por ejemplo un sistema de comunicación por radio que puede ser escuchado por cualquiera que desee hacerlo.

1.2. Algoritmos conocidos [6]

1.2.1. Algoritmo BB84

El esquema de codificación BB84 fue el primer codificador cuántico de información clásica que se propuso de forma que el receptor, legítimo o ilegítimo, pudiese recuperar con un 100% de confiabilidad.

1. La fuente de luz, generalmente un LED o láser, se filtra para producir un rayo polarizado en ráfagas cortas y con muy baja intensidad. La polarización en cada ráfaga se modula por el emisor (Alice) de forma aleatoria en uno de los cuatro estados (horizontal, vertical, circular-izquierdo o circular-derecho).
2. El receptor, Bob, mide las polarizaciones de los fotones en una secuencia de bases aleatoria (rectilíneo o circular).
3. Bob le dice públicamente al emisor que secuencia de bases utilizó.
4. Alice le dice al receptor públicamente que bases se eligieron correctamente.
5. Alice y Bob descartan todas las observaciones en las que no se eligió la base correcta.
6. Las observaciones son interpretadas usando un esquema binario, por ejemplo: horizontal o circular-izquierdo es 0, vertical o circular-derecho es 1.

Este protocolo se complica con la presencia de ruido, el que puede ocurrir en forma aleatoria o ser introducido por una escucha. Con la existencia de ruido las polarizaciones observadas por el receptor pueden no coincidir con las emitidas por el emisor. Para lidiar con esta posibilidad, Alice y Bob deben asegurarse que poseen la misma cadena de bits. Esto se realiza usando una búsqueda binaria con verificación de paridad para aislar las diferencias. Con el descarte del último bit de cada comparación, la discusión pública de la paridad se vuelve inofensiva. En el protocolo de Bennett de 1991 este proceso es:

1. Alice y Bob acuerdan una permutación aleatoria de las posiciones de los bits en sus cadenas, para distribuir aleatoriamente la posición de los errores.
2. Las cadenas se parten en bloques de longitud k, con k elegido de forma tal que la probabilidad de múltiples errores por bloque sea muy baja.
3. Por cada bloque, Alice y Bob computan y anuncian públicamente las paridades. Luego el último bit de cada bloque es descartado.
4. Para cada bloque en el que difirieron las paridades calculadas, Alice y Bob usan una búsqueda binaria con log(k) iteraciones para localizar y corregir el error en el bloque.
5. Para contemplar múltiples errores que aún no han sido detectados, los pasos 1 al 4 son repetidos con tamaños de bloque cada vez más grandes.

6. Para determinar si aún quedan errores, Alice y Bob repiten un chequeo aleatorio:
    a. Alice y Bob acuerdan públicamente una muestra de la mitad de las posiciones en sus cadenas de bits.
    b. Públicamente comparan las paridades y descartan un bit. Si las cadenas difieren, las paridades van a discrepar con probabilidad 1/2.
    c. Si hay discrepancias, Alice y Bob utilizan una búsqueda binaria para encontrarlas y eliminarlas.
7. Si no hay desacuerdos después de n iteraciones, se concluye que sus cadenas coinciden con una probabilidad de error de 2^n.

Ejemplo:

Notación

La siguiente imagen muestra la notación que se seguirá para el ejemplo del algoritmo BB84.

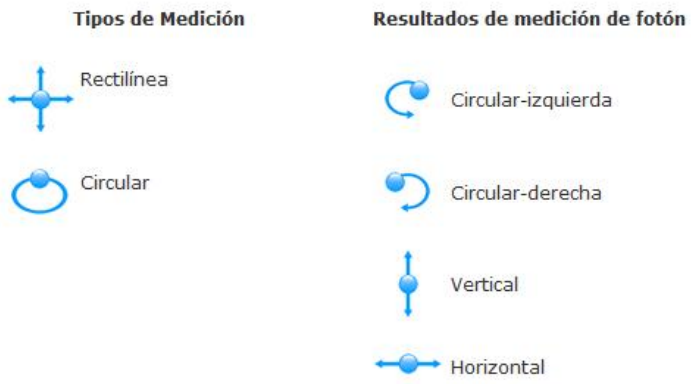

Figura 1. *Notación para el ejemplo de BB84*

Transmisión con escuchas

1. Alice enviará una secuencia de 24 fotones. La probabilidad de que el detector de Bob falle es del 40%.
2. Eve decide aleatoriamente si va a realizar una medición rectilínea o circular para cada fotón que envíe Alice.
3. Por cada medición, existe una probabilidad del 0.4 (40%) de que el detector ni siquiera detecte el fotón.
4. Bob decide aleatoriamente si va a realizar una medición rectilínea o circular para cada fotón que envíe Alice.
5. Bob le dice a Alice a través del canal público qué tipo de mediciones (rectilínea o circular) ha logrado hacer exitosamente, pero no el valor de las mediciones.

6. Alice le dice a Bob, también por el canal público, cuáles de las mediciones fueron del tipo correcto.
7. Como Bob solo va a hacer el mismo tipo de medición que Alice la mitad de las veces, y dado que la probabilidad de que el detector falle en leer un fotón es del 40%, se espera que unos 7.2 de los 24 dígitos compartidos sean utilizables. De hecho en éste ejemplo se generaron 6 dígitos utilizables.

   Bob y Alice quieren saber si alguien ha estado escuchando su comunicación, para lo cual comparten el 50% de los dígitos compartidos. Se va a seleccionar una muestra al azar para que ningún espía pueda predecir que dígitos van a ser verificados y evite modificarlos.
8. Alice revela primero el 50% de sus dígitos.
9. Bob le indica a Alice cual es el valor que midió para los mismos dígitos.
10. Como 2 de los 3 dígitos verificados son incorrectos, Alice y Bob saben que alguien estuvo escuchando su intercambio de fotones.

La siguiente imagen muestra el proceso que se ha seguido y el resultado final.

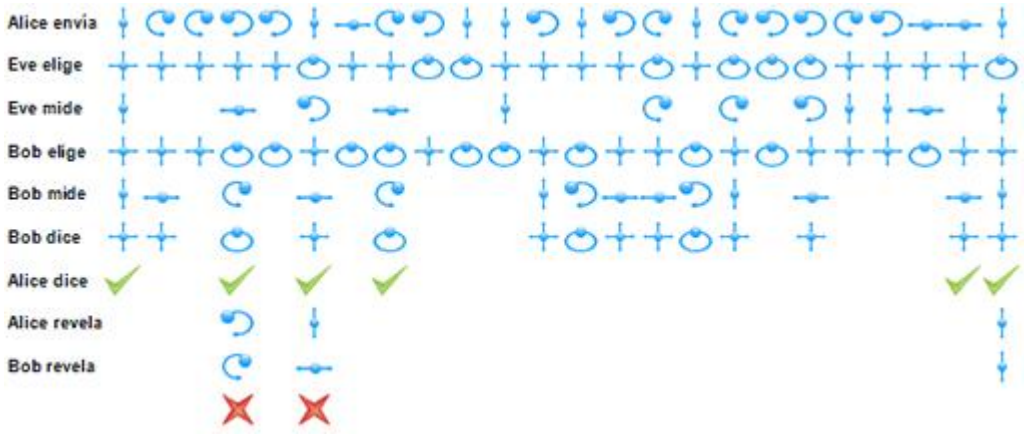

Figura 2. *Mensaje con escuchas para el ejemplo de BB84*

1.2.2. Algoritmo B92

Bennet publicó en 1992 un nuevo protocolo para la generación e intercambio cuántico de claves. Consideramos el mismo sistema anterior pero ahora se escogen como representación de los bits 0 y 1 los estados que aparecen en la siguiente figura.

Bit	Estado
0	$\|\rightarrow\rangle \equiv \|0\rangle$
1	$\|\nwarrow\rangle \equiv \|1'\rangle$

Figura 3. *Bits utilizados para B92*

Alice prepara una cadena de bits aleatorios y prepara los estados a enviar de acuerdo con la figura anterior reflejándose estos en la siguiente figura.

Bits	0	1	1	0	0	1	...
Estados	$\|0\rangle$	$\|1'\rangle$	$\|1'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1'\rangle$	...

Figura 4. *Bits y estados utilizados para B92*

Por su parte Bob genera su cadena de bits para elegir las bases en que realiza sus medidas (0 base +, 1 base ×), pero en lugar de aplicar una medida de von Neuman, Bob aplica ahora a los estados que recibe los operadores de proyección siguientes: Si su bit es 0 (base +), aplica el proyector $P_{not0} = (1 - |0)\ (0|)$. En cambio si su bit es 1 (base ×), aplica el proyector $P_{not1'} = (1 - |1')\ (1'|)$.

El resultado de la aplicación del proyector será cero o uno. ¿Cómo interpretamos los resultados? Si la aplicación de P_{not0} sobre un estado lo deja invariante (autovalor 1), Bob puede estar seguro de que su estado no es $|0)$ y por lo tanto que ha recibido el estado $|1')$, pero si obtiene cero, no puede deducir que estado ha recibido. De forma similar ocurre con el otro proyector.

La estrategia consiste en eliminar de la secuencia los bits en los que Bob ha medido cero, sea cual sea el proyector que ha aplicado, y quedarse con los que ha medido 1. Una vez realizada la secuencia de medidas, Bob debe comunicar a Alice que bits debe desechar y en los demás el acuerdo será total.

2. Objetivos

El objetivo principal de este trabajo fue realizar un cuidadoso y actualizado estudio sobre las técnicas actuales en cuanto a criptografía cuántica, analizando los algoritmos más significativos en el campo. Y una vez realizado, analizar la forma de distribuir claves de una manera cuántica teniendo en cuenta los canales o medios de transmisión. Para todo ello, el estudio estuvo guiado por el profesor tutor de la asignatura Sistemas Operativos Distribuidos (SOD) abordando uno de los puntos del temario relacionado con la seguridad informática que hoy día es uno de los temas importante en informática.

3. Nuevos algoritmos. K05: Un protocolo generalizado de BB84 [1]

En este nuevo protocolo se ha extendido el protocolo BB84 para incluir más de dos estados no ortogonales por símbolo, 1 y 0, basándose en la premisa de que las redes ópticas pragmáticas y los componentes ópticos tales como los filtros de polarización y las fuentes láser no son perfectas. El protocolo K05 ha sido desarrollado en un intento de identificar vulnerabilidades en las redes ópticas cuánticas reales.

Este protocolo, al contrario que el BB84, está basado en dos subconjuntos de estados de polarización, cada uno incluyendo un extenso número de estados para cada símbolo lógico.

Los pasos para la generación cuántica de la clave y la QKD en K05 son:

1. Alice pasa una secuencia de bits binarios, como 100110111011, por un filtro de polarización aleatorio. La asociación de polarización de estados con lógica 1 y 0 son conocidos por Alice solo y desconocidos por cualquier otro, incluido Bob.
2. Bob recibe la secuencia de fotones polarizados los cuales pasan por su filtro de polarización de forma independiente y aleatoria, pero Bob no sabe la asociación entre el valor lógico y es estado de polarización.
3. Los estados de polarización aleatorios de su filtro dejan pasar o rechazan los fotones aleatoriamente polarizados recibidos. Es decir, se genera una secuencia nueva de 1 y 0 lógicos en la cual algunos bits tienen el valor lógico correcto pero no todos.
4. Suponiendo que variando aleatoriamente el filtro de polarización de Bob se generara la secuencia 010110101001 desde la secuencia recibida de Alice. Aunque esta secuencia no es la que Alice transmitió, los bits comunes entre las dos secuencias son importantes aquí. Sin embargo, hasta este paso, ni Alice ni Bob saben que bits son comunes.
5. Bob se comunica con Alice por el canal público y le dice la secuencia de polarización que ha usado mientras recibía los fotones polarizados de Alice. Sin embargo, Bob no revela la secuencia lógica que ha generado.
6. Alice pasa la secuencia lógica que envió a Bob por la secuencia de polarización de Bob. Entonces, Alice compara la cadena inicial de bits con la otra generada desde el experimento e identifica los bits que son comunes en las dos cadenas de bits.
7. Alice le dice a Bob cuales de sus filtros de polarización de estados se usaron correctamente en la secuencia, pero sin decirle su asociación con la lógica de 1 y 0. Los estados de polarización que se usaron correctamente constituirá la clave cuántica.

Las funciones de Caos son candidatas perfectas como generadores de números aleatorios seguros.

4. Distribución de claves cuánticas en el espacio libre (QKD) [3]

Para la investigación de la distribución de claves cuánticas sobre el espacio libre el Institute of Semiconductor Physics de Novosibirsk, Russia ha realizado un experimento. Han utilizado cuatro láseres semiconductores como medio de transmisión. Cada láser genera pulsos de luz con una de las cuatro posibles polarizaciones: 0º, 45º, 90º o -45º. Los rayos láser están combinados con un sistema de espejos en cada rayo, el cual es atenuado por un filtro absorbente en la salida del mismo y es dirigido por un espacio de aire de 70 cm de longitud hacia la unidad receptora. Los láseres semiconductores operan con pulsos de longitud de 8 a 10 ns. Cada láser genera un pulso de luz cuando un pulso de control desde un ordenador se introduce en su fuente de alimentación. Los pulsos del láser atenuados llegan a la entrada de la unidad receptora y son divididos por un espejo divisor de rayos al 50% en dos rayos.

El análisis de la polarización de los fotones se realizó con la ayuda de dos prismas Glan y cuatro detectores de fotones simples como se muestra en las imágenes.

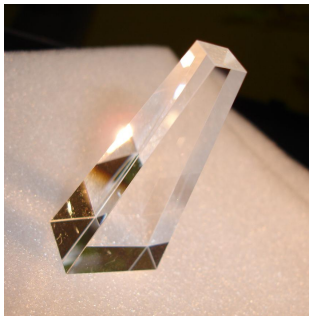

Figura 5. *Prisma de Glan utilizado en el experimento*

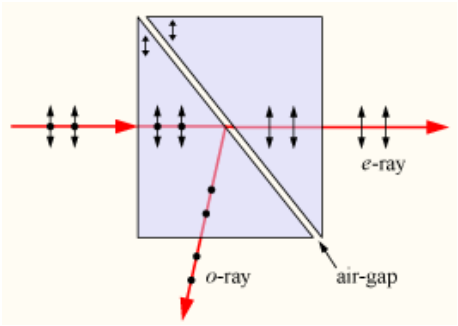

Figura 6. *Gráfica de las características del prisma de Glan*

Figura 7. *Detector de fotones cuántico*

El esquema de la unidad receptora permite ajustar la unidad de transmisión para que, después del atenuador final, cada pulso de láser no suponga más de un fotón y la fracción de pulsos que está conteniendo dos o más fotones sea insignificante. Bajo estas condiciones, la distribución de fotones sobre los pulsos obedecen el estadístico de Poisson.

En criptografía cuántica, una señal se considera una señal de fotón individual si el número medio n de fotones por pulso se encuentra en el rango 0.1-0.2. En particular, con $n = 0.1$, la fracción de pulsos conteniendo dos (tres) fotones es igual al 5% (0.16%) del número de pulsos de fotones individuales. En realidad, en este caso, nueve de cada diez pulsos no contienen fotones. Un fotón (con alguna polarización) enviado por Alice puede llegar a tres fotoreceptores, es decir, un fotoreceptor en su propia base (la división de polarización del prisma no transmite este fotón al segundo fotoreceptor) y dos fotoreceptores en la base externa con igual probabilidad.

En el caso de que las señales de los cuatro fotoreceptores sean detectadas simultáneamente y, además, el número de operaciones simultáneas de dos o más fotoreceptores sea contado, la fracción de pulsos multifotón en la transmisión se podrá calcular con el estadístico de Poisson. El número medio de fotones requerido en los pulsos de luz de la unidad de transmisión se podrá conseguir por medio de la puesta a punto secuencial de la potencia de cada láser.

La seguridad de la transmisión de información está asegurada en el caso de que cada pulso de láser no suponga más de un fotón. Esto se impone como requisito estricto en

los fotodetectores de la unidad de recepción. Estos fotodetectores deberían poseer una alta eficiencia cuántica de detección, ruidos débiles y una tasa de cálculo lo suficientemente alta. Las líneas de comunicación de fibra óptica de los módem funcionan en el rango de longitud de onda infrarroja cercana. En el presente, los mejores detectores de fotones individuales en este rango son los fotodiodos de avalancha.

En este sistema, se utilizaron los fotodiodos C30902S (EG&G), que son los fotodiodos más sensibles en el rango de 0.8 micrómetros y se utilizaron como detectores de fotones individuales. En la siguiente figura se muestra un ejemplo de estos.

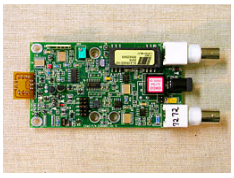

Figura 8. *Fotodiodo C30902S*

Con el objetivo de contar fotones individuales, los diodos de avalancha se conectaron para que operasen en modo Geiger, cuando un fotón puede inducir una avalancha de portadoras de carga. Los diodos se conectaron en un circuito de enfriamiento pasivo. Si un voltaje por encima del umbral de voltaje U(BR) se aplica a través del fotodiodo de avalancha, un fotón que ha llegado al diodo inicia una avalancha de portadoras de carga y la ganancia de los fotodiodos podría estar entre 10^5 y 10^6. La probabilidad de detectar un fotón individual con una longitud de onda de 830 nm será de un 50%. Para decrementar el ruido intrínseco, los diodos se enfriaron a -20ºC usando microrefrigeradores semiconductores Peltier. En la siguiente figura se muestra uno de ellos. La frecuencia de los pulsos de ruido en los fotodiodos de avalancha que están operando en modo Geiger depende de la temperatura y del exceso del voltaje aplicado por encima del valor del umbral.

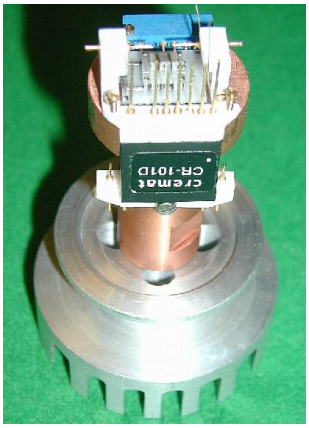

Figura 9. *Microrefrigerador semiconductor Peltier*

En el experimento, la clave cuántica se generó como sigue. El ordenador de Alice especifica la frecuencia de reloj de repetición del pulso láser. Para cada periodo de reloj, se genera un pulso síncrono y se envía a Bob para sincronizar la transmisión y la recepción. Simultáneamente con el pulso de entrada, se alimenta aleatoriamente con un pulso más en uno de los cuatro láseres semiconductores, el cual genera un pulso de luz con una longitud de 10 ns. Los números aleatorios obtenidos con un generador de números aleatorios programable, aunque en el caso general, es preferible usar un generador de números aleatorios basado en procesos de ruido natural.

Cuando Bob recibe un pulso síncrono, adicionalmente genera su propio pulso de entrada con una longitud de 20 ns. Los pulsos de los fotoreceptores se detectaron solo durante el pulso de entrada. Este hecho se necesita para eliminar la mayoría de los pulsos de ruido intrínsecos de los fotoreceptores. Por ejemplo, en número total de pulsos de ruido a una temperatura de -20º y un voltaje de 20V sobre el valor umbral es aproximadamente igual a 3×10^3 por segundo. Al mismo tiempo, el número de pulsos de ruido es aproximadamente igual a *100* por 10^6 pulsos de reloj de la transmisión. La duración de los pulsos de ruido y de fotones individuales desde el fotodiodo después del amplificador se encuentra entre 8 y 10 ns. La adaptación preliminar del tiempo de retardo entre el pulso de entrada y el pulso del fotodiodo de avalancha (operando en virtud de un pulso láser del transmisor) permitió mejorar considerablemente la relación señal ruido y decrementar el número de errores en el código final.

El pulso de salida del fotodiodo de avalancha se consideró a modo informativo solo en el caso en que coincidía el tiempo con el pulso del láser. Todos los ruidos intrínsecos en

el fotoreceptor que no se generaron durante el pulso de entrada se detuvieron del contador de pulsos. Los datos de los cuatro fotodiodos de avalancha se leen por el comando de pulso de sincronización del ordenador de Bob. Si un pulso llega desde alguno de los fotodiodos durante el pulso de entrada, Bob almacena esta información, incluyendo el número del pulso de reloj y generando una señal de pulso para Alice, de acuerdo con esto ella almacena el número del pulso y el láser que está funcionando durante el periodo de reloj dado. Dado que el número medio de fotones por pulso de luz es considerablemente menor que la unidad, no habrá necesidad de almacenar el mensaje entero. Bob elige aleatoriamente las bases de medida de los fotones que han llegado. Si las bases de Bob y Alice coinciden, el próximo número ordinal se asignará al resultado de medida y será almacenado en el fichero de generación de la clave; si no, los datos se rechazarán. De acuerdo al protocolo BB84, este procedimiento lleva a la generación de una clave aleatoria secreta compartida por Alice y Bob.

El tipo de generación de clave dependerá de la frecuencia de reloj de la repetición del pulso láser, el número de fotones por pulso *n* y la frecuencia característica de los fotodiodos de avalancha usados. En este experimento, el tipo de generación de clave estaba limitado por la tasa de datos intercambiada entre el ordenador, el receptor y las unidades de transmisión, a las cuales corresponde una frecuencia de reloj de transmisión de 100kHz.

La generación de la clave cuántica se puede observar en los siguientes datos experimentales. Una vez transmitidos 1^6 pulsos de reloj con n ~ 0.1, se genera una clave cuántica con una longitud de 10721 bits, de los cuales 104 bits (0.97%) parecen estar erróneos (los bits de Alice y Bob no coinciden). Una vez transmitidos con n ~0.2, la longitud de la clave es igual a 18308 bits y 174 bits (0.95%) parecen estar erróneos. Con una frecuencia de 100kHz (usada en el experimento), las longitudes de clave antedichas corresponden a las velocidades de generación de clave de ~ 1 y 1.8 kbit/s, respectivamente. Además, se usó la misma configuración para simular una intercepción no autorizada de todos los fotones por detectores de intrusos y un intento de transmitir a Bob dicha información interceptada. Comparando los códigos obtenidos por el canal público, inmediatamente se descubre que el porcentaje de errores en el código ha incrementado por un factor de varias decenas, lo que indica la presencia de un intruso en la línea de comunicación cuántica.

5. Conclusiones

Con este artículo se ha pretendido realizar un análisis de los primeros y más conocidos algoritmos en criptografía cuántica para la posterior comparación con nuevos algoritmos que se realicen como el que se específica en el mismo. Estos algoritmos son necesarios para el interés final del artículo, que no es otro que dar a conocer la distribución de claves cuánticas (QKD), y más específicamente en este caso, en un medio libre; ésta es una temática de muy alta actualidad y que tiene un futuro investigador de gran calidad e interés.

Por ello, se realizó dicha actividad para la asignatura de Sistemas Operativos Distribuidos (SOD) con el fin de abordar la temática de criptografía en los futuros sistemas computacionales cuánticos, en los que hará falta que la seguridad informática aborde nuevos campos como éste, la criptografía cuántica.

6. Referencias

1. Stamatios V. Kartalopoulos, Ph.D. *Chaotic Quantum Cryptography*. IEEE. University of Oklahoma. EEUU. 2008.

2. Mohammad Amin Amiri; Mojdeh Mahdavi; Sattar Mirzakuchaki. *QCA Implementation of A5/1 Stream Cipher*. IEEE. Iran. 2009.

3. Vladimir L. Kurochkin; Igor G. Neizvestny. *Quantum Cryptography*. IEEE. Institute of Semiconductor Physics. Russia. 2009.

4. Jörgen Cederlöf; Jan-Åke Larsson. *Security Aspects of the Authentication Used in Quantum Cryptography*. IEEE. 2008.

5. Fernandez Delicado, R.; Bellver Cabello, D.; Lloro Boada, I. *The quantum cryptograpy: Communication and computation*. Universitat Politècnica de Catalunya. Spain. 2005.

6. M. Baig. *Criptografía Cuántica*. Universitat Autònoma de Barcelona. Spain. 2001.