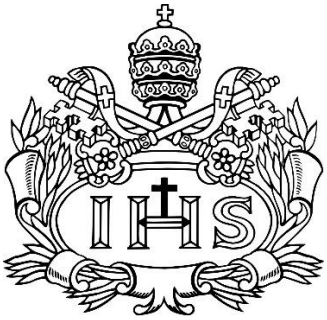
ESTUDIO COMPARATIVO Y EVALUACIÓN DE UTILIDAD DE PROTOCOLOS DE TRANSMISIÓN DE DATOS USANDO CRIPTOGRAFÍA CUÁNTICA

T.G. 1612

SEBASTIÁN LAVERDE ALFONSO

INFORME FINAL



PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA ELECTRÓNICA

BOGOTA D.C.

2016

ESTUDIO COMPARATIVO Y EVALUACIÓN DE UTILIDAD DE PROTOCOLOS DE TRANSMISIÓN DE DATOS USANDO CRIPTOGRAFÍA CUÁNTICA

T.G. 1612

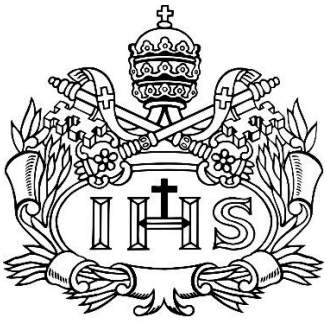
SEBASTIÁN LAVERDE ALFONSO

Trabajo de grado para optar por el título de Ingeniero Electrónico

Director

Edgar Emir González Jiménez, Ph.D

Profesor



PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA ELECTRÓNICA

BOGOTA D.C.

2016

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE INGENIERÍA

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA

RECTOR MAGNÍFICO:	P. JORGE HUMBERTO PELÁEZ P, S.J
DECANO ACADÉMICO:	ING. JORGE LUIS SÁNCHEZ TÉLLEZ
DECANO MEDIO UNIVERSITARIO:	P. SERGIO BERNAL RESTREO, S.J
DIRECTORA DE CARRERA:	ING. ALEJANDRA MARÍA GONZÁLEZ
DIRECTOR DE PROYECTO:	Ph.D, EDGAR EMIR GONZÁLEZ JIMÉNEZ
ASESORA DEL PROYECTO	ING. LUISA FERNANDA GARCÍA VARGAS

ARTÍCULO 23 DE LA RESOLUCIÓN No. 13 DE JUNIO DE 1946

"La Universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado. Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque los trabajos no ataques o polémicas puramente personales. Antes bien, que se vean en ellos el anhelo de buscar la verdad y la justicia".

Dedico este trabajo de grado a:

Mi madre: "La Pioja"

AGRADECIMIENTOS.

En general a toda iniciativa de promulgar la ciencia

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

"La nueva información hace posible las nuevas ideas"
Zig Ziglar, escritor.

La comunicación es una característica intrínseca en el mundo animal, y un sistema complejo y sorprendentemente similar a nuestras conexiones neuronales en el reino vegetal. Cada ser vivo tiene un lenguaje, compuesto por señales que pueden ser de tipos químicas, sonoras, visuales, vibratorias, entre otras, que permiten intercambiar información con el entorno. Existen muchas definiciones de comunicación, siendo una de las más usadas la transmisión de señales a través de un código común, con la que un organismo altera la probabilidad de comportamiento de otro organismo, de modo adaptativo, o bien para el emisor o para ambos, emisor y receptor. Además, la comunicación está conformada por el canal y la información transmitida, la cual puede ser de carácter público o privado, pero en términos prácticos, es el conocimiento explícito de un fenómeno o ente, que en forma de conjunto estructurado de datos relacionados, componen un mensaje con una finalidad y sentido. La información pública, está disponible a cualquier persona en cualquier momento, pero la información privada, también llamada información sensible o confidencial, es aquella en la que difundir un mensaje públicamente, puede suponer un problema para un grupo, afectándolo en diferentes aspectos, según el tipo de información transferida. Por ejemplo cuando se desea dar el número de tarjeta de crédito a un vendedor, esperando que un tercero no intercepte la transmisión. El estudio de la seguridad de la información ha sido siempre una labor muy importante en la historia de la humanidad.

Según la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001 "La seguridad informática consiste en la implementación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio" [1]. La ciencia que estudia las técnicas de codificación para que un mensaje comunicado por un canal inseguro no sea comprensible por una tercera persona a menos que posea la clave, se llama criptografía. La transmisión puede ser utilizada por ejemplo en: llamadas telefónicas, pagos con tarjeta crédito o débito, procesos de extracción de dinero de un cajero, contraseñas en un computador, compras online, mensajes de correo electrónico, archivos de disco duro, registros de una base de datos, entre otros que componen información sensible de un individuo u organización.

En este trabajo se realiza una descripción de los tipos de criptografía (simétrica y asimétrica), presentando su funcionalidad, sus aplicaciones, los posibles ataques o espionaje dentro de la red, esquemas o algoritmos más comunes como el *cuaderno de un solo uso u* OTP[1] y el esquema RSA[2], y los problemas de seguridad relevantes que enfrentan, como el de distribuir la clave privada de manera segura entre los usuarios autorizados; esto con la finalidad de evaluar las bases de la seguridad informática de comunicaciones que tenemos diariamente. También, se valida el algoritmo de Shor teóricamente y por medio de herramientas digitales que permiten hacer simulaciones y ejecuciones en tiempo real sobre procesadores cuánticos. Este algoritmo cuántico usado ahora en criptoanálisis, para factorizar enteros en sus factores primos, demuestra el poder de procesamiento de este nuevo tipo de computación, pensada inicialmente por Richard Feynman, Paul Benioff y Juan Ignacio Cirac; que expone la vulnerabilidad de la seguridad de los sistemas criptográficos usados hoy en día, en especial del RSA.

Además, se describen los fundamentos de la criptografía cuántica y de la distribución cuántica de la clave o QKD[3], que nace como propuesta a un esquema de transmisión de información privada, de modo que su

[1] *One-Time-Pad (OTP)*
[2] Por sus creadores Rivest, Shamir y Adleman
[3] *Quantum-Key-Distribution*

seguridad sea inviolable al estar soportada en leyes físicas fundamentales en vez de alta complejidad computacional o falta de recursos para quebrantarla; se explican sus protocolos más importantes, el BB84 y el E91, que han llevado a las dos más grandes vías de implementación de QKD hoy en día, basadas en *preparar y medir*, y en *entrelazamiento cuántico*. Finalmente, se validan los principios físicos y los circuitos que soportan estos protocolos, y se realiza un análisis comparativo de la eficiencia en la distribución y almacenamiento de las claves generadas por los dos métodos, y redes que actualmente los usan y estudian.

La validación de los dos protocolos se basa en el diseño y prueba de circuitos cuánticos que demuestren los principios físicos que los soportan: el principio de Incertidumbre de Heisenberg, el teorema de no clonación y el entrelazamiento cuántico. Las herramientas digitales a usar son plataformas y simuladores online, iniciativas de empresas como IBM y Google, con el fin que cualquier persona interesada se familiarice con esta nueva tecnología y realice ejecuciones de sus propios algoritmos.

1. MARCO TEÓRICO

1.1. CRIPTOGRAFÍA

La criptografía tiene sus orígenes en la escritura. Proteger lo escrito, mediante su conversión a información cifrada. Uno de los primeros sistemas de cifrado se inventó en Esparta. Consistía en un texto escrito transpuesto sobre una cinta de cuero que se enrollaba alrededor de un bastón, cuyo diámetro era la clave para leer la información en claro (Figura 1). Posteriormente aparecieron otros métodos, como el cifrado *César*, llamado así porque fue usado por Julio Cesar, en el que se usaban técnicas de sustitución entre caracteres del alfabeto para cifrar el mensaje (Figura 2. Esta técnica, junto con la sustitución, constituyen los dos esquemas básicos de cifrado de un mensaje. Estos métodos son actualmente absolutamente inseguros debido al criptoanálisis, que de manera complementaria a la criptografía, es la disciplina que estudia las formas de descifrar comunicaciones encriptadas sin conocer las llaves correctas. Juntas conforman la ciencia de la *criptología*.

Figura 1. Escítala Espartana, transposición.

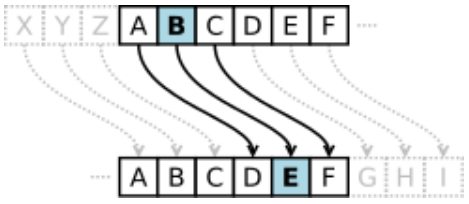


Figura 2. Cifrado César, sustitución.

Los sistemas de codificación moderna tienen sus raíces en tecnología militar. En el siglo XX (siglo de las maquinas) aparece la máquina de cifrar, *Enigma* (1918), utilizada principalmente para comunicar a dos partes interesadas, para que tomen decisiones conjuntas fundadas en información reservada. Sin embargo no fue sino hasta 1948 cuando Claude Shannon estableció las bases de la teoría matemática de la información, fundamentales en la criptología. El desciframiento oportuno era tarea de las mentes matemáticas más brillantes de la época, como la de Alan Turing. El interés del mundo académico por la criptología cobro intensidad alrededor de 1970, cuando se inventaron los criptosistemas de clave pública o asimétrica, formando, junto con la criptografía simétrica, los dos esquemas más usados actualmente.

La codificación y decodificación de un mensaje dentro de la criptografía actual, se realiza por medio de claves o llaves que pueden ser de conocimiento privado o interno en un grupo determinado, o de conocimiento público, es decir, cualquiera puede acceder a ellas. El equivalente de la clave o llave en el mundo digital es el de un algoritmo que ejecuta una serie de operaciones matemáticas sobre el mensaje a transmitir. La criptografía se clasifica según el tipo de clave que usa: privada o pública. También reciben el nombre de criptografía simétrica y asimétrica, respectivamente.

La seguridad de la transmisión del mensaje, puede ser evaluada, para fines de este trabajo, según como cada tipo de criptografía se enfrenta a los siguientes 4 problemas básicos:

1. Distribución de la clave
2. Almacenamiento de la clave
3. Codificación del mensaje
4. Ataques de un tercero

1.1.1. CRIPTOGRAFÍA SIMÉTRICA O DE CLAVE PRIVADA

La criptografía basada en claves simétricas recibe su nombre porque usa la misma clave para encriptar un mensaje y para descencriptarlo. Para que exista una comunicación segura entre dos usuarios remotos por medio de un canal inseguro, ambos deben compartir la misma clave. En primera instancia, para que sea lo más segura posible, debe ser almacenada y distribuida eficientemente, bajo la posibilidad de espionaje. Sin embargo, establecer una clave privada entre ambos usuarios de manera segura, sin que se encuentren físicamente o la transmitan por un canal seguro, es muy difícil. Además, si un usuario desea comunicar un mensaje diferente a varios usuarios, deberá compartir una clave privada diferente con cada uno de ellos, lo que se conoce como el problema de la distribución de la clave.

Una vez distribuida la clave privada, esta será usada una sola vez por cada mensaje y desechada. De modo que si un espía logra conocer información sobre la clave, las próximas transmisiones no se verán comprometidas, ya que esos mensajes estarán codificados con otra clave privada única. El esquema descrito se conoce como cuaderno de un solo uso u OTP (*One-Time- Pad*), como se ilustra en la figura 3:

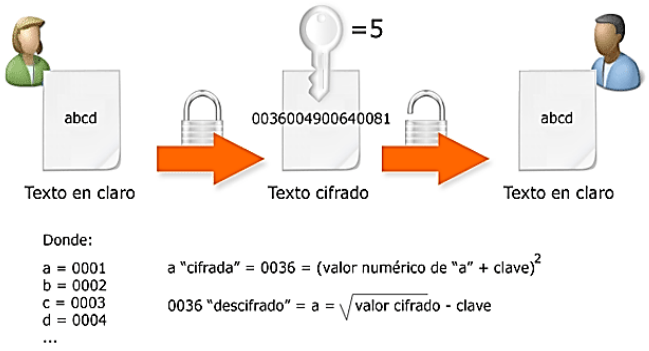


Figura 3. Criptografía simétrica [2].

Esto quiere decir que la clave no deberá ser almacenada por mucho tiempo y que su contenido para encriptar el mensaje, será seguro, porque consistirá en un algoritmo que se usará solo una vez. Por el momento, se puede decir que la clave simétrica se enfrenta con éxito, aunque no total, a los problemas 2 y 3, estipulados al inicio de este capítulo para medir la seguridad de los diferentes tipos de clave, almacenamiento de la clave y codificación del mensaje.

Algunos algoritmos actuales que utilizan criptografía simétrica como el AES[4] o el triple DES[5] realizan varios bloques cíclicos de cifrado en los que combinan operaciones de sustitución y permutación para lograr un mensaje más difuso, dispersando la proporción estadística del mensaje sobre la totalidad del mensaje cifrado.

1.1.2. CUADERNO DE UN SOLO USO Y EL PROBLEMA DE LA DISTRIBUCIÓN DE LA CLAVE

La libreta o cuaderno de un solo uso (OTP), fue inventada por Gilbert Vernam en 1918, y es la prueba de que en la criptografía convencional si existe un código inquebrantable, y que el verdadero problema está en la distribución de la clave privada.

[4] *Advanced Encryption Standard* (2001)
[5] Diseñado por IBM en 1998. Realiza tres vueltas del algoritmo *Data Encryption Standard*.

La seguridad de la clave privada está en la longitud de la misma, ante la gran dificultad de probar todas las combinaciones en un tiempo prudente. Actualmente se consideran seguras claves con una extensión de 128 bits.

Para ilustrar el esquema, se supone que en primera instancia, el primer usuario A convierte el mensaje a su forma binaria y la combina con su clave privada, de la misma longitud, usando una compuerta digital XOR

$$c_i = m_i + k_i \ (mod\ 2) \tag{1}$$

El usuario A transmite ahora el texto cifrado al segundo usuario B por un canal público. Cualquiera, incluyendo a un espía, puede obtener una copia del texto cifrado, pero de nada sirve sino posee información relevante sobre la clave. El usuario B, al que ya se le ha distribuido la clave privada, usa esta para desencriptar el mensaje combinándola con el texto cifrado usando también una compuerta XOR

$$c_i = m_i + k_i \rightarrow m_i + 2k_i = m_i \ (mod\ 2) \tag{2}$$

De esta manera la criptografía simétrica OTP intercambia el problema de la seguridad de la clave, teóricamente 100% segura, por el de distribuir previamente la clave privada entre los usuarios. El OTP puede ser considerado como un código indescifrable para un tercero siempre que los dos usuarios remotos conozcan la clave privada, es decir, que ésta haya sido distribuida. Es imposible de lograr una distribución de la clave simétrica 100% por medios clásicos, sin que los usuarios se encuentren físicamente y la clave se guarde con altísimos estándares de seguridad. Debido a que el usuario A tiene que recurrir a medios de difusión y canales como radiofrecuencia o línea telefónica e Internet, para distribuir la clave al otro u otros usuarios remotos, y estos canales están expuestos a supervisión pasiva, la seguridad de la clave se ve altamente comprometida.

El cuaderno de un solo uso se utiliza para cifrar:

- Mensajes de correo electrónico.
- Archivos de disco duro.
- Registros de una base de datos.
- En general grandes cantidades de datos.

Desventajas:

- Ataque por fuerza bruta: Consiste en intentar cada valor posible de clave privada hasta dar con la correcta.
- Distribución de la clave privada de manera segura: conlleva a ataques de tipo *hombre en el medio*[6], en el que un tercero intercepta la distribución de la clave desde el primer usuario, para conocer la clave y desencriptar el mensaje y/o reemplazarla por su clave privada y hacérsela llegar al segundo usuario sin que ninguno se dé cuenta.

Se puede tener un excelente algoritmo de cifrado pero de nada sirve sino se puede compartir la clave privada entre emisor y receptor del mensaje, es decir, distribuirla. La criptografía de clave pública o asimétrica, por otro lado, se enfrenta con éxito a este problema, basando la seguridad de su transmisión con claves públicas, en complejidad computacional.

[6] *Man-in-the-Middle*

1.1.3. CRIPTOFRAFÍA ASIMÉTRICA O DE CLAVE PÚBLICA

Este tipo de criptografía requiere del uso de dos claves, una clave para cifrar el mensaje y otra diferente para descifrarlo. La clave utilizada para cifrar es de carácter público, mientras que la utilizada para descifrar y poder leer el mensaje permanece privada. Si alguien intercepta el mensaje, porque el canal lo permite, verá la combinación de la clave pública con el mensaje, pero para descifrarla deberá hacer el proceso inverso a la combinación realizada, o poseer la clave privada, como ilustra la figura 4. Es por eso que la operación que ejecute el algoritmo que cifra el mensaje, es decir, que combina la clave pública con el mensaje, deberá tener un inverso cuya complejidad computacional sea razonablemente alta y la clave privada deberá guardarse en medios con altos estándares de seguridad.

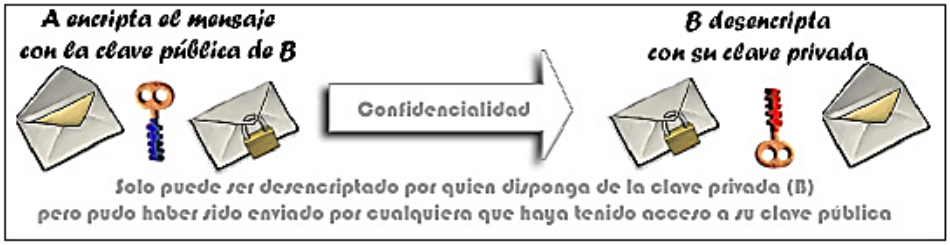


Figura 4. Criptografía asimétrica / Confidencialidad [3].

En este caso el usuario B puede ser una tienda online o un banco, y el usuario A_i pueden ser varias compras o movimientos con tarjeta de crédito o débito de múltiples de usuarios *i* de esa tienda online o banco. Es por eso que la seguridad de la clave depende en gran medida del algoritmo que encripte el mensaje a transmitir. Debido a que la clave que encripta el mensaje es pública, este tipo de criptografía se enfrenta con éxito al problema 1 para medir la seguridad: distribución de la clave; pero la clave privada, usada para desencriptar, deber ser cuidadosamente almacenada.

Se considera que este tipo de criptografía es más segura que la simétrica. Es por eso que protege información u operaciones más delicadas entre usuarios remotos.

La criptografía asimétrica o de clave pública se utiliza para cifrar:

- Llamadas telefónicas
- Pagos con tarjeta crédito o débito
- Procesos de extracción de dinero de un cajero
- Contraseñas en un computador
- Compras online.

Además, la criptográfica asimétrica permite realizar otro proceso fundamental en la comunicación entre partes remotas, la autenticación. Si se cifra un mensaje con la clave privada, cualquiera que posea la clave pública podrá descifrarlo, es decir, todo el mundo. Solo la parte *A* involucrada en la comunicación podrá cifrar, mas todo el mundo podrá descifrar el mensaje. Como la operación de cifrado solo la puede realizar un usuario, éste puede firmar un mensaje de modo que su identidad sea inviolable y el mensaje autentico (Figura 5).

Figura 5. Autenticidad [3].

Descifrar el mensaje con la clave pública equivaldría entonces a verificar la identidad del emisor. Aunque no le añade confidencialidad a la transmisión, el contenido del mensaje se puede considerar más fiable y adquiere la propiedad de *no repudio*[7]

Desventajas de la criptografía asimétrica:

- Fuerza bruta.
- Hombre en el medio: Un tercero sustituye la clave pública del primer usuario por la propia. El segundo usuario cifra el mensaje con la clave pública del espía, por lo que este puede leer fácilmente el mensaje.
- Distribución de la clave pública de manera fiable.

La fiabilidad de un sistema podría entenderse como la probabilidad de que se comporte tal y como se espera de él; en este caso, que la clave pública distribuida sea autentica. Una de las soluciones modernas al problema de distribución de la clave en la criptografía asimétrica son las infraestructuras de clave pública y los certificados digitales CSCP[8], basados en protocolos de autenticidad que aseguran identidad del emisor del mensaje.

La tabla 1 compara las longitudes de las claves de igual resistencia a un tercero que intenta descifrarlas intentando cada valor posible hasta dar con la correcta. Por supuesto, existen esquemas híbridos que combinan criptografía simétrica y asimétrica, principalmente como *pseudo* solución al problema de la distribución de la clave privada y al de la dependencia de la seguridad de la clave pública a los recursos computacionales del espía.

Simétrica o de clave privada	Asimétrica o de clave publica
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

Tabla 1. Comparación: tamaños de claves de igual resistencia a ataques de tipo fuerza bruta [3].

1.1.4. EL ALGORITMO RSA

La seguridad del cifrado asimétrico se basa en el concepto de funciones unidireccionales o de *puerta trasera*. Estas funciones son fáciles con computar en un sentido pero muy difíciles de revertir, a menos que se posea la información de *puerta trasera.* Ejemplo de estas es la exponenciación modular:

$$c = m^e \ mod \ n \tag{3}$$

[7] No poder negar haber firmado un mensaje.
[8] *APICS Certified Supply Chain Professional (CSCP) Certification Program*

donde *m* es el mensaje que se va a encriptar, *e* (encripción), y *n* y la operación que se ejecuta, constituyen la clave pública; y *c* es el resultado de la combinación del mensaje con la clave pública.

Para la operación inversa debemos obtener el mensaje *m* mediante la siguiente operación:

$$m = c^d \ mod \ n \tag{4}$$

El exponente *d*, de descencripción, es la clave privada que permite descifrar el mensaje. Así que las dos operaciones juntas resultan escritas como:

$$m \equiv (m^e)^d \ mod \ n \tag{5}$$

que es equivalente a decir:

$$m \equiv m^{ed} \ mod \ n \tag{6}$$

Para hallar el exponente *d*, que constituye la clave para descifrar el mensaje, se recurre al teorema fundamental de la aritmética, el cual afirma que todo número tiene una única factorización prima. Al ser un problema difícil de solucionar, se puede pensar en la factorización prima de un entero, como una clave secreta.

La figura 6 muestra cuanto se demora un computador en hacer una multiplicación de dos números *p* y *q* Vs cuanto se demora en hallar los factores primos de un número *n*.

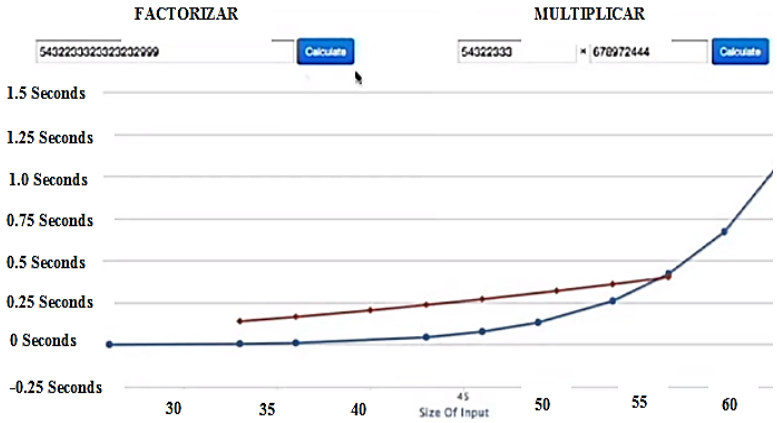


Figura 6. Complejidad temporal multiplicación (rojo) vs factorización prima (azul).

El tiempo de ejecución, al ser exponencial para la factorización, limita la aplicabilidad de los algoritmos clásicos[9], a números con unos pocos cientos de dígitos. El número más grande alguna vez factorizado tuvo 232 dígitos. Se necesitaron aproximadamente 2000 millones de instrucciones por segundo ejecutadas durante un año para lograrlo.

La factorización prima es usada para construir la solución de tipo *puerta trasera.* Si se toman dos números primos aleatorios *p* y *q* de unos cientos de digititos cada uno, y se multiplican obteniendo *n*, este tendrá unos 300 dígitos:

$$n = p * q \tag{7}$$

Gracias a los estudios de Euler en las propiedades de los números, especialmente en la distribución de los números primos, podemos definir a la función $\phi(n)$. Esta función me relaciona los factores primos de *n*, *p*

[9] Que son ejecutados en procesadores cuyo comportamiento físico lo gobierna la mecánica clásica.

y *q*, determinando el número de enteros menores o iguales que *n* que no tienen ningún factor común con *n* mayor que 1. Por ejemplo $\phi(8) = 4$; $\phi(7) = 6$.

Calcular la función $\phi(n)$ es difícil excepto en los casos en los que *n* sea un número primo. Si *n* es un número primo *p*

$$\phi(p) = \mathrm{p} - 1 \tag{8}$$

conduce a un resultado interesante considerando que la función $\phi(n)$ es multiplicativa. Esto es:

$$\phi(p * q) = \phi(\mathrm{p}) * \phi(q) \tag{9}$$

$$\phi(n) = (p-1) * (q-1) \tag{10}$$

Para relacionar este resultado con la exponenciación modular, usamos el teorema de Euler:

$$m^{\phi(n)} \equiv 1 \; mod \; n \tag{11}$$

Lo cual es equivalente a decir que $m^{\phi(n)} mod \; n$ es congruente con $1 \; mod \; n$.

Como $1 \; mod \; n$ es siempre igual a 1 entonces la ecuación (11) también se puede leer como $m^{\phi(n)} mod \; n = 1$.

Ahora si se multiplican ambos lados de la ecuación (11) por *m,* se obtiene:

$$m^{\phi(n)+1} \equiv m \; mod \; n \tag{12}$$

La ecuación (6) se puede reescribir como:

$$m^{ed} \equiv \; m \; mod \; n \tag{13}$$

y con las ecuaciones (12) y (13) se obtiene que $m^{\phi(n)+1} \equiv m^{ed} mod \; n$, es decir:

$$e * d = \phi(n) + 1 \tag{14}$$

Se hace posible calcular la clave privada *d*, si y solo si conocemos $\phi(n)$, es decir la factorización de *n*

$$d = \frac{\phi(n)+1}{e} \tag{15}$$

Se determina un *d*, mediante aritmética modular, que satisfaga la congruencia $e * d \equiv 1 mod \; \phi(n)$. Es decir, se debe hallar un d que sea el multiplicador modular inverso de $e \; mod \; \phi(n)$; o expresado de otra manera, que *e*d-1* sea divisible por $\phi(n)$. Como lo importante es hallar $\phi(n)$, si *n* es un entero muy grande, a un computador clásico le tomaría miles de años descifrar *p* y *q*, ya que utilizaría métodos iterativos como el del algoritmo de Euclides extendido [7] [38] [39].

Este análisis fue publicado independientemente en 1977 por Rivest, Shamir y Adleman. Por eso es generalmente conocida como encriptación RSA de algoritmo de clave pública.

La tabla 2 muestra el progreso de criptoanalistas en la tarea de realizar la factorización prima de enteros en función del número de dígitos

Año	Número de dígitos decimales del entero N	Esfuerzo (MIP años)
1964	20	0,000009
1974	45	0,001
1984	71	0,1
1994	129	5000

Tabla 2. Número de dígitos Vs MIP año [5].[10]

1.2. EL ALGORITMO DE SHOR

Peter Shor, en 1995, propuso un algoritmo cuántico para resolver el problema de la factorización prima en tiempo polinomial en vez de exponencial como lo haría el mejor algoritmo que se ejecute en computadores clásicos [29] [30]. Esta aplicación de la computación cuántica al criptoanálisis de esquemas de criptografía pública tan exitosos hoy en día como el RSA, el algoritmo de Diffie-Hellman, el DSA y ECDSA, es la que más despertó interés al incorporar la cuántica como estrategia para proteger la comunicación entre dos o más partes.

Para descifrar la factorización prima de un entero *N* con un número de dígitos decimales *D* mediante un ataque por fuerza bruta, se escogen todos los primos *p* hasta $N^{1/2}$ y se verifica si *N* es divisible por él o no. En el peor de los casos esto le tomaría a un computador un tiempo aproximado de $N^{1/2}$ operaciones valor que resulta exponencial con respecto al número de dígitos *D*.

Otros algoritmos conocidos son el llamado de criba cuadrática (*QS*), que resuelve la factorización en un tiempo igualmente exponencial en función del número de dígitos, o la criba general del cuerpo de números (*GNFS*) que es el mejor algoritmo clásico conocido hasta el momento para resolver un número en sus factores primos, con crecimiento exponencial en $D^{1/3}$ con respecto al número de dígitos.

En contraste, el algoritmo de Shor logra resolver el problema de factorización en un tiempo que crece polinomialmente en *D*. La versión de Alexey Kitaev que se muestra en la figura 6, fue realizada con 10 qbits (unidad de información cuántica) y tiene un tiempo de ejecución aproximado D^3. La evaluación de complejidad computacional del algoritmo de Shor se explica con mayor detalle en el capítulo de análisis de resultados de este trabajo.

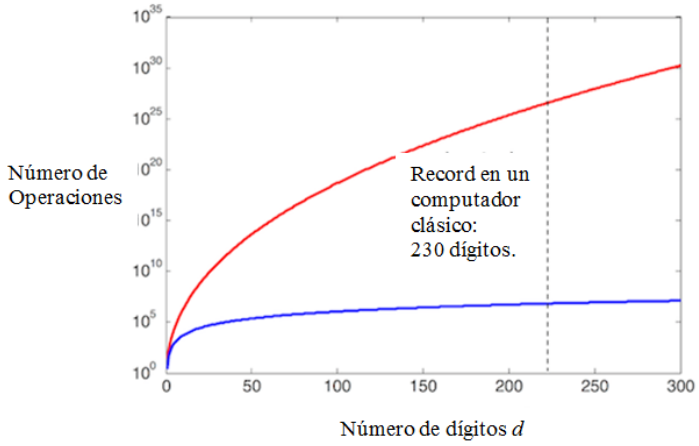


Figura 7. Mejor algoritmo clásico GNFS (rojo) Vs algoritmo de Shor (azul) [6].

[10] MIP es el esfuerzo computacional de un ordenador ejecutando un millón de instrucciones por segundo durante un año.

Para comprender el uso del algoritmo de Shor se considera el problema de encontrar el periodo de una función exponencial modular:

$$a^r \equiv 1 \, mod \, n \tag{16}$$

Siguiendo un análisis similar al de la ecuación (11), debido a que *1 mod n* es siempre igual a 1 para cualquier *n*, $a^r mod\ n$ = 1. Se concluye que:

$$a^r - 1 \;\; sea \, un \, multiplo \, de \, n \tag{17}$$

El entero positivo *r* es llamado periodo de la función. El reto está en encontrar el menor *r* posible, dados *a* y *n*.

Nótese que como ya se dijo en la ecuación (12) es equivalente decir que:

$$a^{r+1} \equiv a \, mod \, n \tag{18}$$

Teniendo en cuenta las ecuaciones (13) y (14) es correcto decir que:

$$a \equiv m \tag{19}$$

$$r + 1 \equiv \phi(n) + 1 \tag{20}$$

La clave privada *d* que desencripta el mensaje, está directamente relacionada con $\phi(n)$ como se ve en la ecuación 14, es decir, con la factorización prima de *n*, la cual a su vez está relacionada con la solución de hallar el periodo *r* de una función de exponenciación modular como la descrita.

Si se fuera a hallar el periodo de la función usando un computador clásico tendríamos que realizar iteraciones de un algoritmo que calcule n/a^{2+i}. Si $\frac{n}{a^{2+i}} = 1$ con un i = 0 entonces el periodo r = 2; de lo contrario se debe incrementar i, hasta que se cumpla (14) y se halle r. Ahora como se había dicho en (5), *n* es igual a la multiplicación de dos primos *p y q*. Valiéndose de algoritmos clásicos conocidos para solucionar el máximo común divisor (*mcd*) entre dos números enteros positivos, como el algoritmo de Euclides [7] [38] [39], calculamos el *mcd* de *n y a*, siendo:

$$2 < a < n - 1 \tag{21}$$

El resultado del mcd (n, a) puede arrojarnos tres resultados diferentes:

$$mcd(a, n) = p \tag{22}$$

$$mcd(a, n) = q \tag{23}$$

$$mcd(a, n) = 1 \tag{24}$$

Si *n y a*, tienen factores primos comunes, entonces el resultado es el más favorable, ya que obtenemos *p o q*, es decir que la ecuación (19) o la ecuación (20) será correcta. De lo contrario *n y a* serán *co-primos*, es decir (21) será correcta. Se repite el cálculo del máximo común divisor hasta que el resultado sea de un r par. Ahora usando la identidad:

$$a^r - 1 = \left(a^{\frac{r}{2}} - 1\right) * (a^{\frac{r}{2}} + 1) \quad (25)$$

El primero de los factores no puede ser múltiplo de n, sin embargo $(a^{\frac{r}{2}} + 1)$ puede serlo o no. Si es múltiplo de n, se debe intentar con otro número a. Si no lo es, entonces podemos hallar los factores primos *p* y *q* calculando el mcd (n, $a^{\frac{r}{2}} \pm 1$).

1.2.1. SUPERPOSICIÓN CUÁNTICA

La tecnología moderna nos ha permitido diseñar y almacenar unidades de información tan diminutas que millones de ellas cabrían en una célula. La unidad más pequeña de información es el *bit*, que permite representar dos valores diferentes (como abierto/cerrado o verdadero/falso) y asignar dichos valores al estado de encendido (1) o apagado (0). Su equivalencia física es la del estado de un transistor que permite o no el flujo de electrones entre sus terminales. Con el avance tecnológico, se ha hecho posible el diseño de componentes cada vez más pequeños, hasta llegar a tamaños equivalentes a unos cuantos átomos (*14 nm*).

A escalas nano-métricas los electrones que definen el estado del transistor, empiezan a experimentar fenómenos físicos como el tunalamiento cuántico, que no pueden ser explicados por la mecánica clásica. Es también debido a fenómenos cuánticos, que la posición de un sencillo fotón al difractar un cristal birrefringente[11], esté descrito por una función probabilística. Ambas partes puede incluso interferir entre sí de la misma manera que interfieren las ondas, como lo demuestra el famoso experimento de Young [8], donde un sencillo electrón, al pasar por una doble rendija, se comporta como una onda, es decir, pasa por las dos rendijas e interfiere consigo mismo, creando un patrón de interferencia. Esto permite que computacionalmente se hagan varias operaciones de manera paralela.

En computación cuántica la unidad fundamental es el *qbit*. El comportamiento de sus estados puede ser descrito por la función de onda, y su evolución por la ecuación de Schrödinger. Una medición significa un colapso de la función probabilística en alguno de los estados de la base, en nuestro caso, |1> y |0>[12]. La probabilidad de que una medición colapse en determinado resultado está determinada por la regla de Born. En este orden de ideas, un sistema cuántico puede ser descrito por el diagrama de la figura 8.

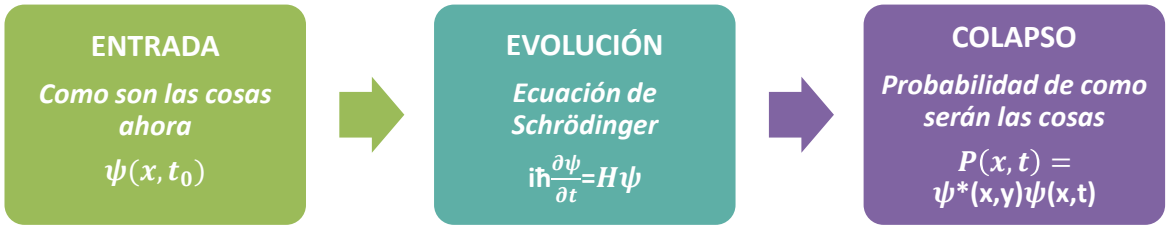


Figura 8. Flujo de un sistema cuántico

Los *1s* y *0s* son la representación binaria de una propiedad del electrón o el fotón, como el *spin* o la *polarización*, sujetas a principios cuánticos. Antes de realizar una medida sobre el electrón para determinar el valor de la propiedad, esta puede tomar ambos valores 1 y 0, dada la aleatoriedad intrínseca de los sistemas cuánticos.

[11] Birrefringencia o doble refracción es una propiedad óptica de ciertos cuerpos, especialmente el espato de Islandia, que consiste en desdoblar un rayo de luz incidente en dos rayos linealmente polarizados de manera perpendicular entre sí como si el material tuviera dos índices de refracción distintos: la primera de las dos direcciones sigue las leyes normales de la refracción y se llama rayo ordinario; la otra tiene una velocidad y un índice de refracción variables y se llama rayo extraordinario. Ambas ondas están polarizadas perpendicularmente entre sí.

[12] Notación de Dirac [9]

Como el estado del qbit antes de ser medido no es un valor discreto sino una superposición, se suele representar usando la esfera de Bloch (Figura 9), la cual es una representación geométrica del espacio de estados puros de un sistema cuántico de dos niveles. Ver anexo sobre circuitos cuánticos.

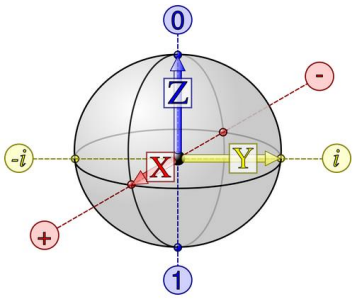


Figura 9. Esfera de Bloch [10].

Con estados cuánticos, si 5 qbits de información, obtengo 2^5 → 32 configuraciones diferentes, de las cuales se pueden usar una a la vez para hacer una operación. Pero si son 5 qbits de información, se pueden realizar 32 operaciones paralelas antes de realizar una medida que colapse el sistema cuántico en una de las configuraciones con una probabilidad dada. Esto se conoce como superposición de estados cuánticos y establece la superioridad en cálculo de un procesador cuántico respecto a uno clásico.

La evolución del sistema cuántico, es manipulada mediante compuertas cuánticas. Estas a diferencia de las compuertas lógicas convencionales (AND, OR, XOR) son de carácter reversible[13]. Toda compuerta cuántica puede ser representada por una matriz unitaria Hermitiana[14]. Antes de la medición, la función de onda representa matricialmente la esperanza matemática[15] del estado cuántico. Ver anexo 1 sobre circuitos cuánticos.

Ahora bien, el algoritmo de Shor usa el paralelismo cuántico y la interferencia constructiva, para determinar el periodo de objetos aritméticos de la misma manera que los físicos han usado la dispersión e interferencia de ondas electromagnéticas para determinar la periodicidad de una red cristalina determinando cierta propiedad global de la función.

El circuito cuántico total del algoritmo de Shor se ilustra en la figura 10. Está basado en el algoritmo de Simon para encontrar el periodo de una función vectorial booleana [11] [12]:

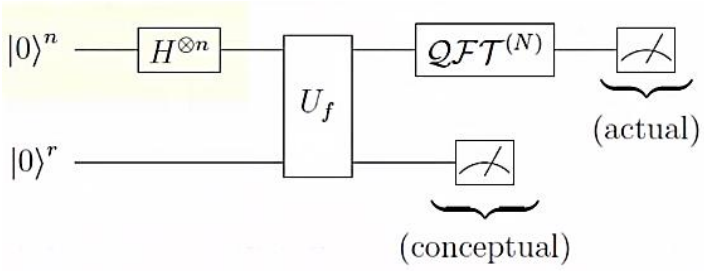


Figura 10. Circuito cuántico del algoritmo de Shor

[13] Una compuerta lógica cuyo número de salidas (información de salida) sea igual al número de entrada (información de entrada) será reversible (no disipativa); la información permanece invariante, lo cual lleva consigo una energía manifiestamente constante. Una compuerta de este tipo es capaz de realizar una operación lógica susceptible de que en ella se invierta el proceso de cómputo y al final se recupere las condiciones iniciales sin pérdida alguna de energía.

[14] Los auto valores propios (*eigen*) de las matrices Hermitianas siempre son números reales, y por lo tanto una matriz Hermitiana es capaz de representar cantidades físicas reales.

[15] También llamada valor esperado de una variable aleatoria real, es un número que de alguna manera nos releja cierta información acerca de la distribución de la misma.

Donde la compuerta Hadamard $H^{\otimes n}$ prepara *n* qbits en paralelismo cuántico o superposición. Estos evolucionan con un oráculo, cuya función es ayudar a determinar si el resultado de una prueba determinada es aceptable o no[16] (la exponenciación modular cuántica). La transformada cuántica de Fourier (QFT) es un operador que sirve para establecer una medida del espectro en frecuencia de la función, directamente relacionado con el periodo de la misma. Ver anexo 1 sobre circuitos cuánticos

Su resolución es similar a la del circuito de Simons, considerando que cada medida siempre resulta en valores propios, y que debido a la naturaleza probalística de los estados cuánticos, se deben realizar varias vueltas del algoritmo para lograr la solución.

Se requiere una transformación unitaria U_f que aplica la función multiplicación modular

$$x \rightarrow ax \; mod \; n \tag{26}$$

Los valores propios de esta función están relacionados con el periodo de *a mod n*. Valores que puede ser hallados usando el algoritmo de estimación de fase cuántica.

Estos valores deben ser medidos con la mayor exactitud posible para poder determinar el periodo. Para ello se ejecuta varias veces el algoritmo. También se aplica el operador unitario a una variable

$$\text{b} = a^2, a^4, a^8, a^{16} \; mod \; n \tag{27}$$

Parando en b = a^{2^p} donde $2^p \approx n^2$. Este operador tendrá los mismos vectores propios que (23), y sus valores podrán ser determinados de forma simultánea. Los valores propios de la trasformación unitaria de *a* son de la forma $e^{i\phi}$. Así que si $b = a^2$, sus valores propios serán de la forma $e^{2i\phi}$. ϕ podrá ser calculado con una precisión aproximada de 2^{-p} donde

$$\phi = \frac{2\pi k}{r} \tag{28}$$

De modo que el algoritmo de Shor, precisa de un circuito cuántico que implemente la multiplicación modular y de otro que implemente la QFT o algoritmo de estimación de fase cuántica. Existen varios circuitos lógicos que implementan la exponenciación modular, pero no equivalen a transformaciones unitarias con el carácter de reversibilidad. Se precisa de circuitos cuánticos de exponenciación modular de la forma expresada en la ecuación (26).

Si fuéramos a llamar a una subrutina clásica que calcule la multiplicación modular debemos primero replantearla ya que un algoritmo cuántico podrá usarla solo si esta compilada en una secuencia de compuertas cuánticas tipo Toffoli o CNOT para hacerla reversible. Actualmente la implementación de la multiplicación modular cuántica requeriría aproximadamente

$$\#n^2 = numero \; de \; compuertas \; cuanticas \tag{29}$$

Donde *#n*, el número de dígitos binarios usados para representar al entero n. En [6] y en el capítulo de protocolo de pruebas se encuentra un mayor análisis sobre el algoritmo de Shor.

[16] Idealmente es un método que provee las salidas esperadas de cada caso de prueba dado.

1.3. CRIPTOGRAFIA CUÁNTICA Y QKD

Las primeras ideas sobre la criptográfica cuántica fueron discutidas por Stephen Weisner en 1983, quien propuso dos modalidades de comunicación que no eran posibles por medio de la física clásica: un canal de *multiplexación cuántica* y un billete infalsificable. Sin embargo, no recibieron mucha atención ni aceptación en la comunidad científica hasta diez años después con Peter Shor y las primeras implementaciones que validaban el funcionamiento de esquemas de criptografía cuántica.

La meta era lograr tareas imposibles o intratables con criptografía convencional de la misma manera que un computador cuántico aprovecha las leyes de la física para enfrentarse con éxito a problemas cuya solución es de alto grado de complejidad. Su práctica se ha enfocado con grandes avances a tratar uno de los problemas a los que se enfrenta la seguridad de los sistemas de comunicación, el problema de distribuir la clave privada, naciendo así distribución de clave cuántica o QKD. Otras aplicaciones incluyen protocolos cuánticos para el *compromiso de bit* y *lanzamiento de moneda cuántica*[17]. Hoy en día hay gran variedad de implementaciones de computación cuántica y de QKD, y existen sistemas comerciales disponibles en el mercado.

El QKD se presenta como solución al problema de la distribución de la clave y usa las leyes de la física más esquemas como OTP para hacer la comunicación invulnerable a espías. Los dos tipos de criptografía descritos anteriormente, simétrica y asimétrica, están sujetos a supervisión pasiva, es decir, espionaje del canal usado sin que el emisor del mensaje ni el receptor se den cuenta de ello, sea que estén distribuyendo la clave o compartiendo el mensaje encriptado. Por eso ambas técnicas deben recurrir a protocolos que aseguren a legitimidad del mensaje y su confidencialidad. En el esquema de compartir secretos cuánticamente (QSS)[18], tales perturbaciones involucradas por un tercero espiando la transmisión, indetectables en un canal clásico, constituyen la acción de medir un sistema en la mecánica cuántica, donde ciertas propiedades físicas son complementarias. Esto quiere decir que toda tentativa de supervisión dentro del canal cuántico provoca necesariamente cambios detectables en la señal. Lo anterior se conoce como el *principio de incertidumbre de Heisenberg*, el cual a su vez soporta al teorema de no clonación cuántica.

1.3.1. TEOREMA DE NO CLONACIÓN CUÁNTICA

Este teorema fue concertado por Wooters, Zurek y Dieks en 1982 y enuncia lo siguiente:

"Un estado cuántico arbitrario no podrá ser duplicado perfectamente"

La prueba de esto se encuentra sustentada en resultados directos de la linealidad de la física cuántica, y está relacionada directamente con otro importante teorema que afirma que si una medición, permite adquirir información sobre un sistema cuántico, entonces el estado de ese sistema se verá necesariamente alterado.

Usando la imposibilidad de clonación se pueden diseñar esquemas para distribuir la clave que van a compartir dos usuarios de manera incondicionalmente segura. Sin embargo, este teorema también imposibilita el uso de técnicas de corrección de error clásicas en las que se hacen copias de respaldo de un estado cuántico en la mitad de un procesamiento computacional. Peter Shor y Andrew Steane, en 1995,

[17] *Bit commitment y Coin Tossing o Coin flipping*
[18] *Quantum Secret Sharing*

fueron los primeros en desarrollar códigos correctores de error cuántico para superar problemas de decoherencia y defectos en componentes usados en los circuitos cuánticos.

Adicionalmente cabe destacar que este teorema reafirma el teorema de NO teleportación clásica, muy diferente a la teleportación asistida por entrelazamiento, cuya aplicabilidad ha sido demostrada y será discutida posteriormente.

1.3.2. PRINCIPIO DE INCERTIDUMBRE DE HEISENBERG

Este principio estipula que hay ciertos aspectos o propiedades de las partículas subatómicas que no podemos conocer con precisión simultáneamente. Según esto, intentar medir el valor de la posición de una partícula con él más alto grado de exactitud, incrementará la incertidumbre en poder medir la cantidad de movimiento de la misma partícula con la misma exactitud. El límite de la precisión con la que se puede medir las cosas está determinado por la constante de Planck

$$\Delta x * \Delta P_x \geq \frac{h}{4\pi} \tag{30}$$

Esta incertidumbre es intrínseca del sistema cuántico, se deriva del hecho de medir, mas no del instrumento de medida.

Una comunicación de este tipo podría reemplazar a los certificados CSCP, ya que dos usuarios remotos, podrían transmitirse información reservada con seguridad absoluta avalada por las leyes físicas de la naturaleza, sin que inicialmente hayan compartido algún secreto.

1.3.2.1. LA POLARIZACIÓN DEL FOTÓN

La dirección de oscilación del fotón es una propiedad cuántica de la luz, conocida como *polarización*. Pueden distinguirse tres tipos de polarización según la dirección de oscilación del campo eléctrico con respecto al eje de propagación[19] (Figura 11):

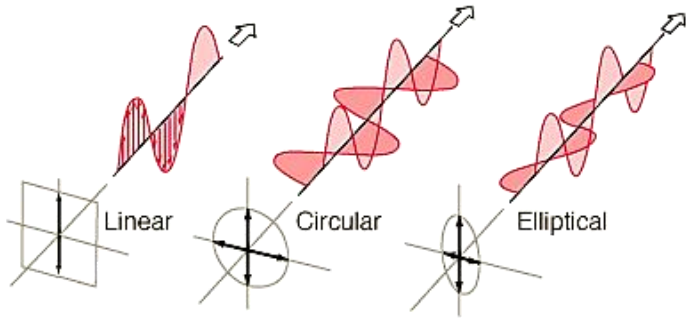


Figura 11. Polarización de la luz según oscilación del campo eléctrico [13].

Si la polarización del fotón es de tipo lineal, podremos distinguir entre 4 polarizaciones con respecto a la del cristal

[19] *La luz es una onda electromagnética transversal, pero la luz natural por lo general no está polarizada, todos los planos de propagación son igualmente probables. Si la luz está compuesta de dos ondas planas de igual amplitud pero con una diferencia de fase de 90°, entonces se dice que la luz está polarizada circularmente. Si las dos ondas planas tienen diferente amplitud y están desfasadas entre sí 90°, o si el desfase es distinto de 90°, la luz se dice que está polarizada elípticamente* [13].

1. Horizontal → 0º con respecto a la polarización del cristal.
2. Vertical → 90º con respecto a la polarización del cristal.
3. Diagonal (+) → 45º con respecto a la polarización del cristal
4. Diagonal (-) → 135º con respecto a la polarización del cristal

Un fotón incidente en un cristal se comporta de forma distinta en función de su polarización con respecto a la del cristal. Un haz de luz ordinario está compuesto por muchos fotones con polarizaciones diferentes. Si luz con polarización oblicua atraviesa un cristal de calcita, éste repolarizará los fotones al azar en polarización horizontal o vertical (Figura 12).

El comportamiento más aleatorio se da cuando la polarización de la luz está en una base diferente a la del cristal que atraviesa, por ejemplo: si la polarización de la luz es de tipo horizontal o vertical, y la del cristal birrefringente, de tipo diagonal (Figura 13). El 50% de los fotones saldrán con polarización (+) y el otro 50% con (-). Esto quiere decir que un fotón individual con polarización diagonal tendrá 50% de probabilidad de culminar polarizado horizontalmente o verticalmente, antes de medirlo el fotón se encuentra en una superposición de estos dos estados de polarización.

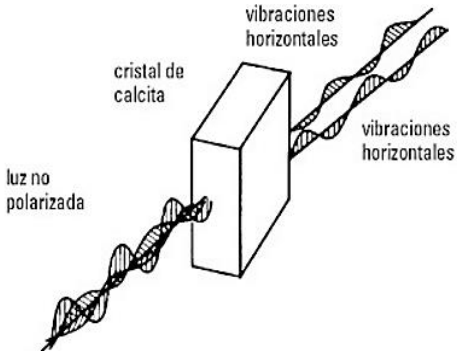


Figura 12. Cristal polarizador a luz no polarizada [28]

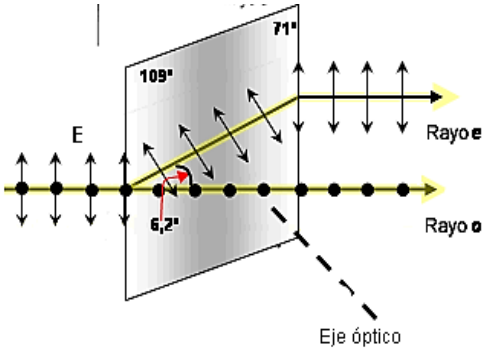


Figura 13. Cristal polarizador a luz polarizada [28]

Los fotones que inciden con polarización horizontal atraviesan directamente el cristal y los de polarización vertical experimentan una deflexión que los desplaza sobre el eje de propagación. Este fenómeno se conoce como birrefringencia de los materiales. De esta manera crean los filtros de la polarización rectilínea.

De la misma manera, si se hace una rotación de 45º o 135º sobre el cristal de calcita, se estarán haciendo mediciones o filtros en el eje diagonal de polarización. Por lo que si incide un fotón con polarización horizontal, este tendrá 50% de probabilidad de atravesarlo con polarización diagonal (+) o diagonal (-).

Las mediciones de la polarización del fotón de tipo rectilínea y diagonal conforman las propiedades físicas complementarias gobernadas por una desigualdad como la presentada en la ecuación (30), y son la base para los primeros sistemas criptográficos cuánticos.

Dicho esto, en QKD, dos usuarios que quieren compartir un secreto, obtienen unos estados cuánticos y posteriormente los miden. A partir de allí, se comunican por un canal clásico para determinar cuáles qbits de los resultados de las mediciones son útiles para generar una clave privada; los otros qbits se descartan mediante un proceso llamado *cernimiento/destilaciónón* (*sifting)*. Luego ejecutan corrección de error y describen mediante un parámetro de seguridad, que cantidad de información está comprometida, es decir, cuanto sabe el espía. Si esta cantidad es debajo de cierto umbral, no se puede garantizar la seguridad en la clave, ni por ende, en el mensaje que se encriptará con ella; generalmente se aborta la comunicación. Si el parámetro está por debajo del umbral de seguridad establecido, se puede aplicar amplificación de la

privacidad para eliminar cualquier información obtenida por el espía. La variable que establece el umbral se conoce como QBER (*Quantum Bit Error Rate*). Las comunicaciones clásicas deben ser autenticadas para evitar ataques de tipo hombre en el medio.

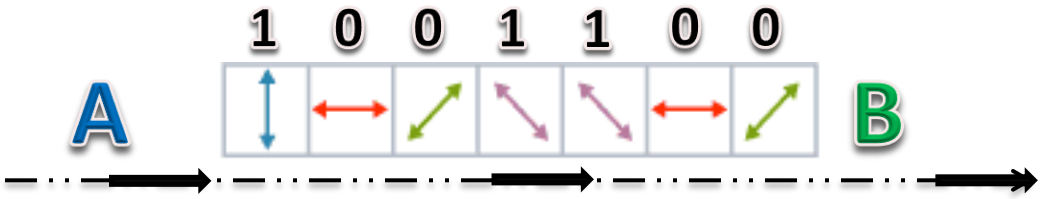
1.3.2.2. PROTOCOLO BB84

Llamado así porque fue desarrollado teóricamente inicialmente por Charles Bennet y Gilles Brassard en 1984. Este físico y criptógrafo retomaron las ideas de Weisner para estudiarlas, culminando con la demostración de un prototipo experimental para establecer la viabilidad tecnológica del concepto de criptografía cuántica. Su finalidad era permitir que A y B, usuarios remotos, pudieran compartir una clave aleatoria secreta, generada de la manera más segura y fiable posible usando distribución de clave cuántica, sustentada en el principio de incertidumbre de Heisenberg, más la técnica de criptográfica simétrica, el cuaderno de un solo uso OTP, para posteriormente utilizarla en la transmisión de información reservada.

En los protocolos de criptografía cuántica también se usa un canal clásico para comparar las señales enviadas por el canal cuántico, verificando la presencia de espías en la comunicación, y así tomar decisión sobre la información que está o no comprometida.

El esquema funciona de la siguiente manera

1. Para comenzar a crear la clave, el primer usuario A envia y registra una serie de bits a B, generados aleatoriamente, usando la codificacion según la polarizacion lineal del fotón mostrada anteriormente (0º y 90º para rectilinea, 45º y º135º para diagonal) y por medio de un canal cuantico que puede ser fibra optica u espacio libre, el cual esta gobernado por las leyes de la fisica cuántica (Figura 14):



Canal Cuántico: espacio libre o fibra óptica

Figura 14. Transmisión de cadena de fotones de polarización aleatoria de A a B.

2. Para cada fotón, o bit, en la recepción de B se aplica un filtro polarizador aleatoriamente y se registra el resultado (Figura 15):

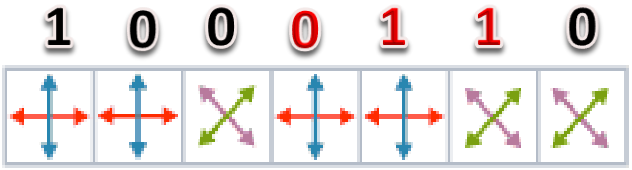


Figura 15. Tipo de filtro Usado por B.

Según la el principio de incertidumbre, se introducirán errores en los bits, debido a que algunos de los filtros no corresponde al tipo de polarización original de la transmisión A → B. Los fotones que pasen el filtro polarizador con la orientación incorrecta tendrán un 50% de probabilidades de terminar con su valor lógico contrario, como es el caso de los bits 1 y 3 en el registro del resultado de la medición de B.

Si un tercero E tratara de espiar la transmisión, las leyes de la física cuántica le prohibiría usar los dos tipos de filtros polarizadores al mismo tiempo (Figura 16), y tendría que elegir aleatoriamente uno para

cada medición, por lo que se introduciría un error similar al introducido por la medición de B. En análisis de resultados, se detalla la dinámica de la tasa de error de bit cuántico o QBER.

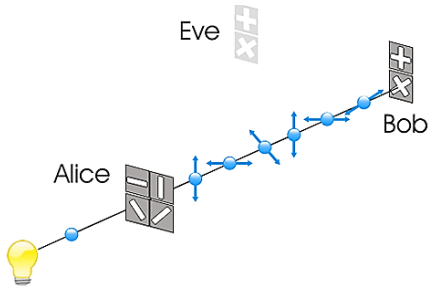


Figura 16. Espionaje [14].

3. Para crear la clave o llave cuántica y además confirmar intentos de espionaje, el usuario B le comunica a A, por medio de un canal clásico, los tipos de filtros polarizadores que él eligió aleatoriamente (Figura 17):

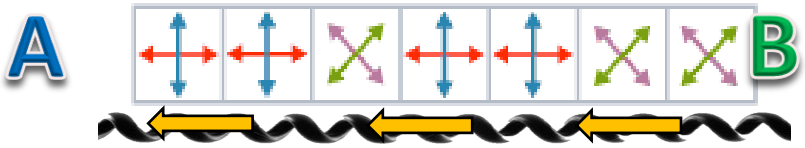


Figura 17. Comunicación clasica del tipo de filtro usado.

y el A le comunica cuales elecciones fueron correctas y no deberían presentar error, a menos que un espía E estuviera interceptando la transmisión (Figura 18):

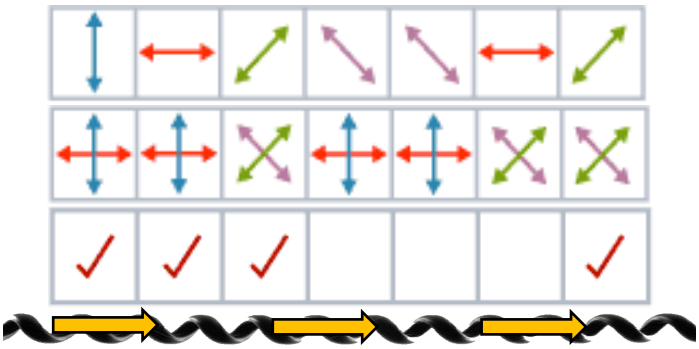


Figura 18. Coincidencias.

4. Los dos usuarios A y B conservan solo los eventos donde los bits fueron detectados con la base correcta, y pasan la información almacenada como estados cuánticos, a una cadena de bits, como se observa en la figura 20:

Figura 20. Cadena generada.

Según esto la clave cuántica generada (con la podrían comenzar a encriptar la información), es el código 1000 que en decimal es el número 8. Antes de tomar el 8 como la clave, y usarla como cuaderno de un

solo uso, se debe confirmar que no hubo espionaje en la transmisión. Para hacer esto sin comunicar la clave por un canal inseguro, se pueden usar técnicas con las que se cierne o se destila (*sifting).* Por ejemplo: técnicas de comparación de paridad[20] entre los registros de A y B; técnicas de *reconciliación de la información y amplificación de privacidad*, y en general algoritmos cuánticos de corrección de error, que permiten lograr un acuerdo incondicionalmente seguro (QSS) por medio de un canal público. Si el resultado de la evaluación de paridad de A difiere de la del usuario B, y se supera un umbral de QBER, no se alcanzan los parámetros de seguridad, se aborta la comunicación y la clave generada se considera insegura.

Es importante rescatar que debido a las propiedades intrínsecas de los canales y a las características de la generación y recepción del rayo de fotones, se introducirán errores adicionales que pueden hacer que un 0 se mida como un 1 o viceversa, así se use el filtro polarizador correcto. Por eso es tema de estudio las mejores maneras de hacerlo, de amplificar la información reservada, y de corregir los errores introducidos en la transmisión.

Un ejemplo de una cadena generada por estos medios, con espionaje dentro del canal cuántico, es registrado en la tabla 3.

Bits aleatorios de A	0	1	1	0	1	0	0	1
Bases aleatorias de A	+	×	+	×	×	+	×	+
Polarizacion de A	→	↖	↑	↗	↖	→	↗	↑
Bases aleatorias de E	+	+	×	×	+	×	×	+
Polarizacion que mide y envia E	→	→	↗	↗	↑	↗	↗	↑
Bases aleatorias de B	+	×	×	×	+	×	+	+
Polarizacion de B	→	↗	↗	↗	↑	↗	→	↑
Clave privada compartida	0	0		0				1
Error por espia E	✓	✗		✓				✓

Tabla 3. Ejemplo de generación de clave privada BB84

Donde observamos que debido a las características de la supervisión dentro del canal cuántico, es fácil determinar un umbral que indique el nivel de seguridad de la transmisión.

La naturaleza de la clave, conformada por direcciones de polarización de fotones sencillos, hace que sea complejo almacenarla por mucho tiempo, sin que se presenten errores en la clave de algunos de los dos usuarios. Además cuanto más tiempo han de conservarla, más es vulnerable a espionaje.

El protocolo BB84 para distribución de clave cuántica sumado al OTP, conforman un sistema criptográfico que se enfrenta con éxito a los problemas 1 y 3, estipulados al inicio del capítulo 1, para medir la seguridad de los diferentes tipos de clave; distribución de la clave y codificación del mensaje a transmitir. Debido al esquema OTP, el almacenamiento de la clave, aunque muy importante, no comprometerá la seguridad de la transmisión de mensajes posteriores, debido a será una clave de un solo uso.

Es posible diseñar un sistema criptográfico, basado en correlaciones cuánticas, que se enfrente con éxito total al problema de distribución y almacenamiento de la clave. Este sistema nace con la versión de David Bohm del célebre efecto Einstein-Podolsky-Rosen (EPR) [15].

[20] Contar el número de 1 y de 0 en una cadena de bits.

1.3.3. EL EFECTO EPR

En 1991 el físico Arthur Eckert concibió un sistema de criptografía cuántica distinta, basada en el efecto denominado EPR, concebido en las predicciones contra intuitivas del fenómeno de acción a distancia, que fueron inicialmente discutidas en 1935 por Albert Einstein, Boris Podolsky y Nathan Rosen. Este efecto tiene lugar cuando un átomo con simetría esférica, emite dos fotones en direcciones contrarias [15]. El estado de polarización inicial de cada fotón es indefinido. Solo cuando se midan bajo la misma base, se obtendrán resultados siempre opuestos. En la figura 9 se muestra un ejemplo en el que los usuarios A y B miden con filtros de polarización rectilínea al par de fotones que surgen entrelazados. Ambos tienen la misma probabilidad de registrar un 1 o un 0, pero inmediatamente el primer usuario registre un 1 en su medición, es 100% seguro que el usuario B registrará un 0 en la suya.

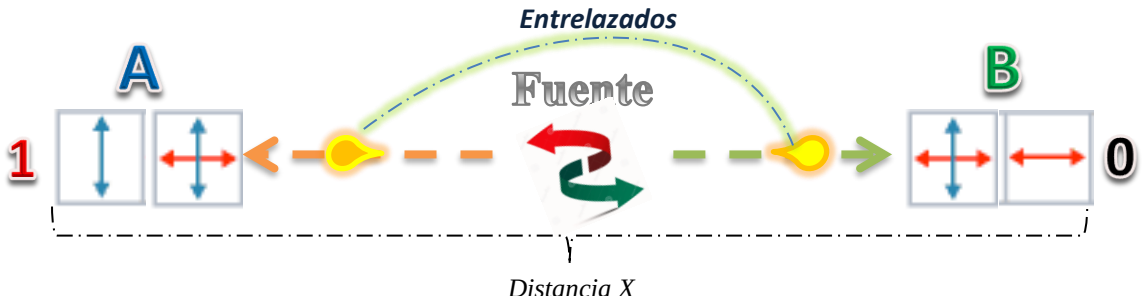


Figura 21. Medición de polarización rectilínea sobre par fotónico entrelazado.

Lo valioso de este efecto, es que la polarización queda determinada para ambos fotones, sólo cuando se efectúa una medición en alguno, por más alejados que se encuentren, como si fueran un sistema inseparable y probabilístico, cuyo colapso hará que sus partes decaigan en extremos contrarios de la base. Tal parece ser que la información cuántica se puede transmitir inmediatamente sin importar que tan lejos estén sus elementos entrelazados, violando aparentemente, límites físicos como el de la velocidad de la luz. Esta acción a distancia inmediata es uno de los efectos más extraños, sorprendentes, y poderosos de la mecánica cuántica El concepto de entrelazamiento cuántico también se puede extender a otras propiedades de partículas fundamentales como la dirección del spin del electrón.

1.3.4. ENTRELAZAMIENTO CUÁNTICO

Fue Erwin Schrödinger el primero en utilizar el término entrelazamiento para describir las correlaciones entre dos partículas que interactuaban y se separaban como en el experimento EPR. El entrelazamiento cuántico es usualmente creado a partir de interacciones entre partículas subatómicas de varias formas, pero no son sujeto de este trabajo. Este fenómeno físico cuántico es la base para crear otro tipo de sistema criptográfico, y para nombrar conceptos como la teleportación cuántica.

Si se tienen dos sistemas cuánticos que no están interactuando A y B, el espacio del sistema compuesto podría ser descrito por su producto tensorial $|\psi>_A \otimes |\psi>_B$. Estos estados se conocen como estados de producto, y pueden ser separables o no [15]. Si el estado no es separable se dice que es un estado entrelazado. Si el sistema compuesto se encuentra en uno de estos estados, no es posible atribuirle a ninguno de los dos sistemas un estado puro definido. Un ejemplo de un estado entrelazado puede ser uno de los 4 estados de Bell [16].

$$\frac{1}{\sqrt{2}} (|0>_A |0>_B + |1>_A |1>_B) \tag{31}$$

1.3.4.1. ESTADOS DE BELL

Los estados de Bell, concebidos por el físico John S. Bell, son estados entrelazados cuánticamente, cuyas correlaciones no pueden ser explicadas clásicamente por ninguna teoría de variables locales ocultas. El entrelazamiento cuántico viola la desigualdad CHSH, establecida en 1969 por John Clauser, Michael Horne, Abner Shimony, y Richard Holt, que establece un límite para sistemas clásicos anti-correlacionados, cuantificando matemáticamente las implicaciones planteadas teóricamente en la paradoja de Einstein-Podolsky-Rosen y permitiendo así su demostración experimental.

Si tenemos dos sistemas entrelazados A y B, a los que se les efectúa dos tipos de mediciones diferentes A_1,A_2 y B_1 , B_2, con posibles resultados +1 o 0 como se ilustra en la figura 22:

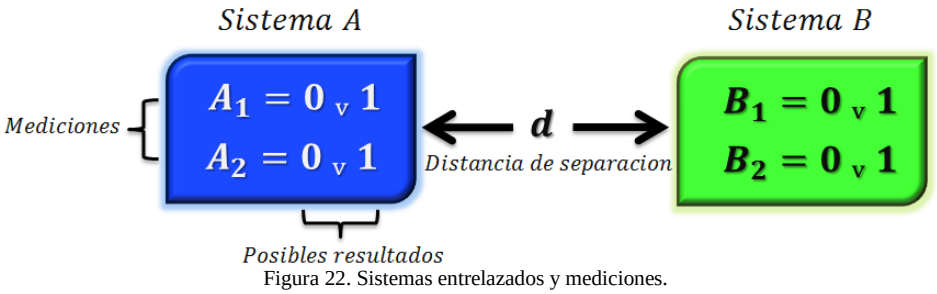


Figura 22. Sistemas entrelazados y mediciones.

Según [6], el resultado del valor absoluto de C debe ser menor o igual a 2, donde C es

$$C = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \tag{32}$$

$$|C| \leq 2 \tag{33}$$

donde el valor esperado de la correlación $\langle AB \rangle$ está dado por

$$\langle A_{1,2} B_{1,2} \rangle = P(1,1) + P(0,0) - P(0,1) - P(1,0) \tag{34}$$

Esta famosa desigualdad ha sido demostrada cierta en numerosos sistemas clásicos. En general debe serlo si la teoría que rige los sistemas correlacionados, obedece los principios *de realismo y localidad* que afirman

- *Realismo:* Todos los observables tienen un valor definido independientemente del tipo de medición efectuada.

- *Localidad:* Ningún tipo de información puede viajar más rápido que la velocidad de la luz. Debe por lo tanto existir una variable oculta que defina todas las correlaciones $\langle AB \rangle$, relacionada a la distancia ***d***.

Sin embargo, en sistemas entrelazados cuánticamente por estados como el de Bell,$|C| > 2$ es decir, los principios de realismo y localidad no deben ser válidos en el mundo cuántico. Es por esto que podemos tener partículas cuánticas entrelazadas entre grandes distancias, donde una perturbación a cualquiera de ellas afectará inmediatamente a su par entrelazado.

1.3.4.2. PROTOCOLO E91

El esquema funciona de la siguiente manera:

1. El primer usuario A, genera pares de fotones entrelazados bajo el efecto EPR, envía uno de los fotones de cada par y guarda el otro para sí mismo. Algunas modificaciones a los esquemas sugieren que la fuente generadora sea una tercera persona remota. Lo importante es que las partículas estén preparadas en estados cuánticos entrelazados y que cada usuario reciba una de cada par.

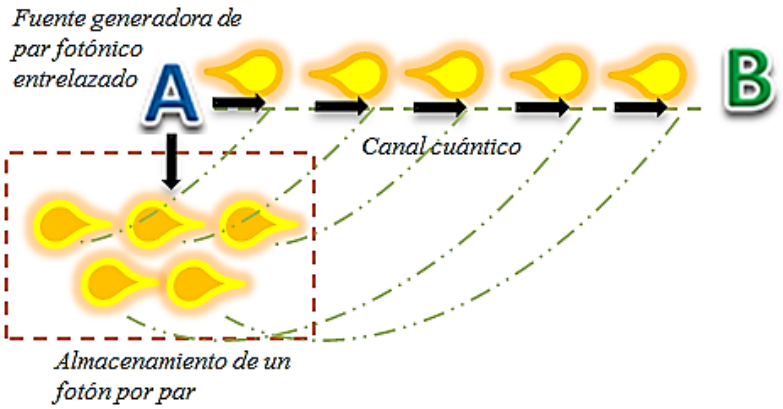


Figura 23. Generación de par fotónico entrelazado.

2. Ambos usuarios remotos almacenan los fotones sin medirlos y justamente cuando la clave va a ser utilizada, cada uno procede a medir algunos de sus fotones aleatoriamente entre las bases lineales: rectilínea y diagonal, para comprobar si alguien más está espiando la transmisión. Si no existe espionaje, el usuario B siempre obtendrá un 0 cuando A obtenga un 1 y viceversa como muestra la figura 9, siempre que ambos midan en la misma base, es decir, el 50% de la veces. Con los qbits cuya medición fue coincidente se crea la clave privada.

   Cuando se obtenga la clave privada definitiva, el registro de B será el de A negado por lo que pueden acordar compartir un secreto. Si un tercero intenta espiar la transmisión y mide fotones en bases aleatorias, si están no coinciden con la base usada por A y B, se introducirán errores en la mitad de los bits comprometidos como se ha analizado anteriormente. Un ejemplo podría ser que el espía use bases circulares o elípticas para su medición cuando A y B usan rectilínea.

3. Si se detecta espionaje dentro de la transmisión, se analiza que cantidad está comprometida. Si se puede reducir la información que conoce el espía, se ejecutan algoritmos de corrección de error cuántico, y así se aumenta la seguridad en la clave. Una técnica muy usada en protocolos de este tipo, es la *purificación por entrelazamiento cuántico*. Si no se detecta, los usuarios pueden medir los fotones restantes para crear la clave que se utilizará en la encripción del mensaje. La transmisión y uso de la clave pueden darse siguiendo esquemas como el OTP.

La idea es cambiar la transmisión de qbits desde el usuario A al B (paso 1 en BB84), mediante un canal cuántico, por el de transmitir qbits entrelazados desde una fuente común a ambos usuarios, uno a cada uno.

Si la fuente productora de fotones fuera confiable, podría emitir dos qbits en el mismo estado de alguno de los 4 lineales (0º, 45º, 90º y 135º), para que luego los usuarios los midan aleatoriamente en alguna de las dos bases lineales (rectilínea o diagonal), como se representa en la figura X. La fuente común luego anuncia públicamente los estados enviados para que A y B conserven solo los qbits donde hubo coincidencia de bases. Esto sería equivalente al protocolo BB84, pero en vez de confiar en una fuente (que

puede estar en manos del espía), el protocolo de Eckert asume dos qbits emitidos en un estado de entrelazamiento máximo como uno de los estados de Bell. Entonces cuando A y B

Este protocolo, intercambia el problema de almacenar de manera segura una clave ya estipulada por mediciones con diferentes polarizadores, por el problema de almacenar estados cuánticos sin medirlos, es decir, en un estado de superposición o estado coherente[21]. En el protocolo BB84, la clave debe ser almacenada clásicamente hasta que se va usar. Así que, aunque fue creada incondicionalmente segura, su seguridad al pasar el tiempo solo será tan grande como la seguridad del su almacenamiento. Con el método EPR, los usuarios podrían potencialmente almacenar los estados entrelazados sin medirlos, para luego hacerlo y crear la clave privada justo antes de que la vayan a usar como cuaderno de un solo uso, eliminando por completo el problema 4 al que se enfrentan los distintos tipos de criptografía, el almacenamiento de la clave.

Las ideas básicas de los protocolos BB84 y E91 son sencillas, aunque contra intuitivas, sustentadas en una matemática lejos de la complejidad de esquemas criptográficos como el RSA, y cuya seguridad puede ser demostrada incondicionalmente segura, bajo efectos cuánticos como la superposición de estados, el principio de incertidumbre de Heisenberg, el entrelazamiento cuántico y con teoremas como el de la no clonación cuántica. Por otro lado, para aplica QKD en la práctica se necesita establecer un límite superior para la cantidad de información que conoce el espía, dada la tasa de error cuántico (QBER) y otros parámetros.

1.3.5. TASA DE ERROR DE QBIT Y LA DESTILACION DE LA CLAVE PRIVADA

Es claro el poder y las posibilidades que abre este tipo de tecnología. Sin embargo, QKD no elimina la necesidad de otros elementos primarios en la criptografía, como la autenticación. Dentro del canal cuántico también existe ruido, por eso, para que exista un acuerdo incondicionalmente seguro entre las dos partes, se recurre a técnicas como la *reconciliación de información*, *amplificación privada y purificación por entrelazamiento cuántico.* En QKD, luego de que los usuarios acuerden qué bits son seguros y cuáles deben ser descartados, realizan corrección de error y establecen que cantidad de información puede tener un espía sobre su comunicación. Se muestra el siguiente diagrama en bloques (Figura 24) que describe el proceso de QKD:

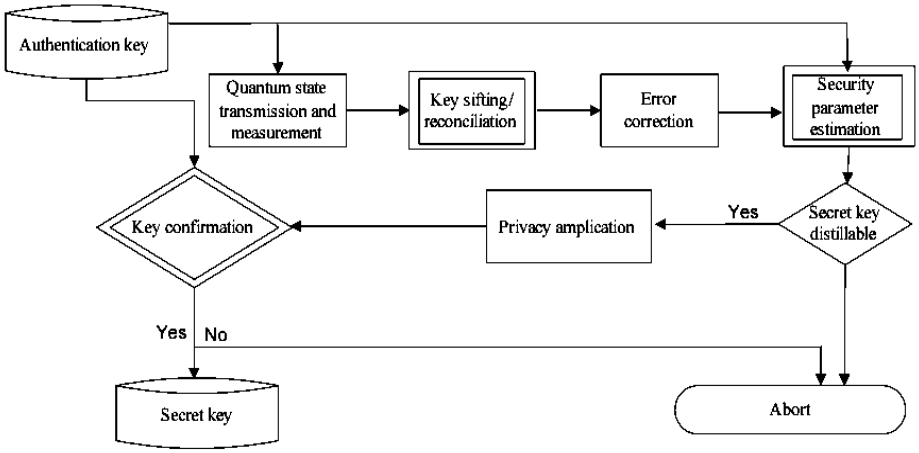


Figura 24. Diagrama de bloques de destilación de la clave QKD [18].

[21] Se llama estado coherente o se habla de coherencia cuántica para referirse a un estado cuántico que mantiene su fase durante un cierto periodo de tiempo. El mantenimiento de la coherencia cuántica hace posible fenómenos de interferencia y el entrelazamiento [17].

El error en los qbits, provenientes de diferentes fuentes, incluyendo al espía, es uno de los parámetros de seguridad más importantes en criptografía cuántica y en QKD, ya que establece la relación entre los qbits enviados y los errores detectados en ellos. Mediante la evaluación de la tasa de error de qbit, o QBER, se establece el umbral límite que separara las claves seguras de las inseguras. Para determinar el valor máximo del QBER admisible se hace un examen de la información que comparten los usuarios remotos A, B y el espía E [19]:

$$Informacion\ compartida\ entre\ A y\ B \rightarrow I(A,B)$$

$$I(A,B) = H(A) - H(A|B) = H(B) - H(B|A) \tag{35}$$

$$I(A,E) = H(A) - H(A|E) = H(E) - H(E|A) \tag{36}$$

$$I(B,E) = H(B) - H(B|E) = H(E) - H(E|B) \tag{37}$$

Donde $H(X)$ es la entropía de Shannon[22], y $H(X|Y)$ es la entropía condicional[23]. De las ecuaciones se deduce:

$$I(A,B) + I(A,E) \leq 1 \tag{38}$$

Por otro lado se puede afirmar que la información compartida por A y B debe ser mayor o igual que el máximo de la información mutua entre A y E y B y E:

$$I(A,B) \geq MAX\{I(A,E), I(B,E)\} \tag{39}$$

Con las ecuaciones (37) y (38) se concluye que:

$$I(A,B) \geq 0{,}5 \tag{40}$$

Ahora expresando la información compartida entre A y B es equivalente, en términos del QBER a

$$I(A,B) = 1 - [(QBER * \log_2 QBER) - ((1 - QBER) * \log_2(1 - QBER))] \tag{41}$$

Debido a las ecuaciones (40) y (41) se establece el límite para el QBER [18]:

$$QBER \leq 0{,}11 \tag{42}$$

Se recuerda que en un canal cuántico, toda supervisión es activa, se refleja como perturbaciones en los bits y en un aumento en el QBER, que puede significar un crecimiento por fuera del umbral establecido como error seguro en la clave, por lo que será descubierta inmediatamente se realice el espionaje. Si el error permanece menor al umbral establecido por la ecuación (42), se puede realizar amplificación privada de la información para reducir cualquier información restante que el espía pueda tener. Si el error es superior al QBERmax, se aborta la comunicación y no se puede garantizar seguridad en la clave y/o mensaje compartido.

Las transmisiones realizadas por canales clásicos, deberán estar autenticadas para evitar ataques del tipo hombre en el medio. También es importante resaltar que cada componente involucrado en los sistemas y

[22] Mide la incertidumbre de una fuente de información [20].

[23] Si en vez de tener una única variable aleatoria X, existe otra variable Y dependientes entre sí, es decir el conocimiento de una (por ejemplo, Y) entrega información sobre la otra (por ejemplo, X). Desde el punto de vista de la entropía de la información podemos decir que la información de Y disminuirá la incertidumbre de X. Por tanto, podemos decir que la entropía de X será condicional a Y [20]

redes que usan criptografía cuántica, tienen probabilidad de fallo y error intrínseca a ellos mismos. Las etapas realizadas para destilar la clave privada más segura posible pueden dividirse en:

1. Autenticación: A y B anuncian públicamente una parte aleatoria de la clave en bruto (entre un 5% y un 10%). Estos bits se sacrifican. Se aconseja un umbral de error (R=tasa de error) máximo de un 11%.

2. Unificación de la clave: A y B dividen los bits restantes en subconjuntos. Para cada cadena calculan la paridad descartando cada vez el último bit 1, b2, …, bL} calculan la paridad P= b1 b2 … descartando cada vez el último bit de la cadena (para evitar que E obtenga información). La paridad se enuncia públicamente. Si coinciden, entonces guardan la cadena. Si no, entonces localizan y borran el bit erróneo, dividiendo la cadena en dos partes y repitiendo el proceso cada vez, en aquél subconjunto en el que las paridades salgan distintas. Al final, con alta probabilidad A y B comparten la misma cadena de bits.

3. Amplificación de la privacidad: Se reduce la información de E. Ejemplo: se toman dos bits de clave. Imaginemos que E sabe que uno está bien, por ejemplo el primero. Se sustituyen estos dos bits por la paridad (XOR) de los dos. La información de E desaparece porque depende del segundo bit, que ella desconoce. Este proceso reduciría a la mitad el número de bits de la cadena [21].

El tamaño de la clave a la salida del proceso de destilación, es independiente del tamaño inicial y del QBER inicial. Este comportamiento se debe a las funciones de amplificación de la privacidad[24] .

[24] Funciones Hash [22].

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Analizar los protocolos BB84 y E91 para generación, protección y distribución de claves para transmisión segura de datos y detección de espías basada en criptografía cuántica, para su implementación en tareas de transmisión segura de información.

2.2. OBJETIVOS ESPECÍFICOS

1. Verificar el algoritmo de Shor para su implementación en detección de claves públicas basadas en el sistema criptográfico RSA.

2. Comparar la funcionalidad de los protocolos BB84 y E91 y su eficiencia para generar claves cuánticas y confrontarlos en aspectos como error en la información compartida y cantidad conocida por un espía.

La criptografía cuántica requiere el uso de tecnología muy costosa: uso de fuentes fotónicas fiables que produzcan el desplazamiento de un solo fotón y logren entrelazar un par de ellos; altísimas tasas de muestreo en componentes digitales, circuitos ópticos y filtros polarizadores, entre otras cosas que no están al alcance para el desarrollo de este trabajo. Debido a esto, la comprobación de los protocolos y algoritmos se basa en verificar los principios que los hacen posible, con el fin de que, se realice un análisis comparativo de seguridad entre los tipos de criptografía: simétrica, asimétrica y cuántica (por dos métodos).

La estrategia para el cumplimiento de los objetivos está basada en investigación y diseño de circuitos cuánticos que demuestren el funcionamiento del algoritmo de Shor y de los principios físicos en lo que se basa la criptográfica cuántica. Según esto, el trabajo de grado se divide en 3:

2.3. OBJETIVOS DE DISEÑO

A. Diseñar un circuito cuántico que verifique el algoritmo de Shor.

B. Diseñar un circuito cuántico que valide el principio de incertidumbre de Heisenberg.

C. Diseñar un circuito cuántico que demuestre el fenómeno de entrelazamiento cuántico.

Las ejecuciones deben ser prueba suficiente de los fenómenos y principios de la mecánica cuántica que hacen posible la criptografía cuántica, principalmente los protocolos usados para generar y distribuir la clave privada entre dos usuarios remotos y el algoritmo de Shor usado para romper la seguridad del esquema popular RSA. Los diseños tienen que ser al menos simulables por alguna herramienta digital.

3. DESARROLLO

3.1. DESCRIPCIÓN

El trabajo pretende realizar una investigación acerca de las tecnologías actuales asociadas a la generación y distribución de claves publicas usando criptográfica cuántica, centrándose en los protocolos de mayor uso como el BB84 y el E91. Durante el desarrollo del proyecto habrá tres agentes ficticios involucrados en la comunicación: *A, B y E* (por *espía*); encargados de generar una clave pública segura y de espiar la transmisión de datos. La totalidad del trabajo puede ser desglosado en dos grandes fases o bloques, destacando que pueden existir fases de desarrollo posteriores a este trabajo.

FASE I: Algoritmo de Shor: Después realizar una contextualización teórica, enfocada en la seguridad informática de comunicaciones que tenemos diariamente, y en la seguridad informática que brinda la mecánica cuántica, se valida el algoritmo de Shor teóricamente y por medio de herramientas digitales Este algoritmo cuántico para factorizar enteros grandes en sus factores primos, demuestra el poder de procesamiento de la computación cuántica. En parte como justificación para el proyecto, con la validación del algoritmo de Shor, se realiza una comparación en términos de complejidad computacional y velocidad de ejecución con algoritmos clásicos usados en la resolución del sistema de encriptación RSA. El resultado de esta fase justificara la existencia de protocolos cuánticos para comunicaciones con altos requerimientos de seguridad.

FASE II: ***Protocolos de generación de clave cuántica:*** Con la descripción de los fundamentos de la criptografía cuántica y de la QKD, y de sus protocolos más importantes, el BB84 y el E91, que han llevado a las dos más grandes vías de implementación de QKD hoy en día, basadas en *preparar y medir*, y en *entrelazamiento cuántico*, se validan los principios físicos mediante circuitos que los soporten, y se realiza un análisis comparativo de la eficiencia en la distribución y almacenamiento de las claves generadas por los dos métodos. Se investiga de redes de comunicación que actualmente los usan y estudian.

La validación de los dos protocolos se basa en el diseño y prueba de circuitos cuánticos que demuestren los principios físicos que los soportan: el principio de Incertidumbre de Heisenberg, el teorema de no clonación y el entrelazamiento cuántico. Las herramientas digitales a usar son plataformas y simuladores online, iniciativas de empresas como IBM y Google, con el fin de que cualquier persona interesada se familiarice con esta nueva tecnología, y realice ejecuciones de sus propios algoritmos. Ver anexo sobre circuitos cuánticos.

En esta fase se llevara a cabo la mayor parte del análisis necesario para la resolución del objetivo principal. El resultado de estas ejecuciones será comparado en aspectos como porcentaje error en la transmisión de datos y cantidad “escuchada” por el agente involucrado *E*, para definir qué sistema sería más conveniente para implementar una red de distribución de claves y para ofrecer servicios de seguridad informática.

Continuamente se concertará que redes existen actualmente usando este tipo de tecnologías e inferiremos en las razones de optar por uno u otro de los protocolos. Describiremos a las empresas que se dedican a estos altos estándares de seguridad, con ánimos de poder contactar a alguna o a un grupo de investigación en criptográfica cuántica, para proyectar el porvenir del uso de esta tecnología.

La figura 25 representa el flujo de procesos, separados por fases de desarrollo, para cumplir con el objetivo general del proyecto. Los procesos en medio de las dos fases serán desarrollados en paralelo junto con la ejecución de los otros.

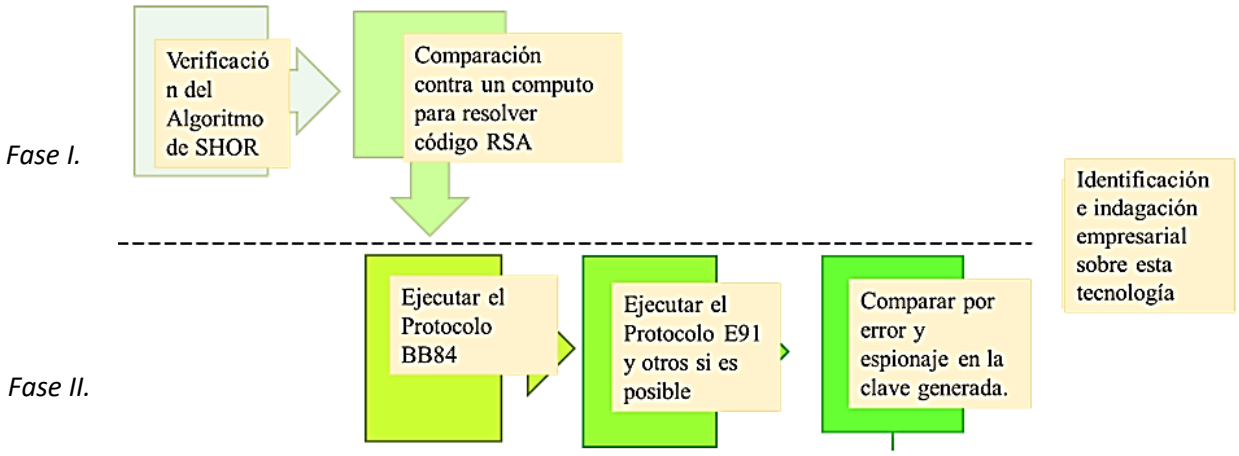


Figura 25. Flujo de procesos

3.2. TECNOLOGÍA UTILIZADA

3.2.1. IBM QUANTUM EXPERIENCE

IBM Quantum Experience representa el nacimiento de la computación cuántica en la nube[25], ofreciendo acceso práctico a la computación cuántica experimental, basada en qbits superconductores y uniones Josephson. Es programada usando resonancia magnética nuclear. Es la herramienta principal del trabajo de grado debido a que es la única que permite hacer ejecuciones en procesadores cuánticos reales y no solo simulaciones dentro de cómputos clásicos.

QASM 2.0 es el lenguaje que especifica los circuitos cuánticos de esta plataforma, y el *compositor* es la interfaz gráfica que permite construirlos y medirlos. Para describir y procesar el trabajo completo, las entradas de los circuitos y las salidas de medición están integradas, usando alguna forma de API[26] coordinada a través de un lenguaje de nivel superior. Esta herramienta también realiza la corrección de errores cuánticos (QEC). QEC permite cálculos arbitrariamente largos utilizando componentes defectuosos. Sin embargo, la tasa de error por operación de puerta debe estar por debajo de un umbral de 10E-4. Para mayor detalles consultar [23].

El *IBM Quantum Experience* le permite a cualquier usuario:

- Correr algoritmos y hacer experimentos y ejecuciones en procesadores reales de IBM.
- Trabajar con qbits individuales.
- Incorporar alrededor de 10 compuertas cuánticas.
- Explorar tutoriales y simulaciones ideales sobre lo que podrá hacerse con la computación cuántica.

[25] Procesamiento y almacenamiento masivo de datos en servidores que alojen la información del usuario. El usuario tiene acceso "instantáneo" a sus datos y en todo momento.
[26] Interfaz de programación de aplicaciones.

Fue lanzada el 4 de Mayo del 2016 para cualquiera interesado en tener fácil acceso a procesadores cuánticos de IBM. Puede ser ejecutada en cualquier dispositivo de escritorio o móvil con acceso a Internet. El procesador cuántico está compuesto por 5 qbits superconductores y está instalado en el *IBM T.J Watson Research Center* en Nueva York. La topología de la red del dispositivo se muestra en la figura 26. Debido a ella, algunos circuitos que deben ser re-diseñados mediante el uso de compuertas tipo SWAP. Ver anexo sobre circuitos cuánticos.

Los qbits están hechos de metales superconductores sobre un chip de silicio y pueden ser diseñados y producidos usando los métodos convencionales de fabricación de estos chips. Los diseños de los circuitos cuánticos, en aplicaciones como las mediciones de paridad usadas en protocolos de corrección de error cuántico, pueden escalar a dimensiones más grandes y volverse sistemas cuánticos más complejos, pero las simulaciones y ejecuciones están limitadas a 5 qbits.

Las señales son transmitidas hacia adentro y fuera de un refrigerador de dilución criogénica que mantiene al procesador cuántico en un ambiente a temperaturas tan bajas que llegan a 15 milikelvins (Figura 27). De esta manera se llevan a cabo las operaciones en el procesador, con ingeniería robusta tanto a nivel del dispositivo como a nivel de control electrónico para que el desempeño de los experimentos realizados por los usuarios sea el más óptimo y confiable.

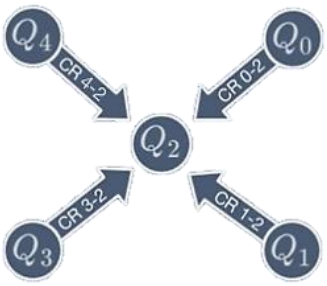


Figura 26. Topología de la red del procesador cuántico de IBM.


Figura 27. Cables coaxiales usados para transmitir al/desde el interior del refrigerador.

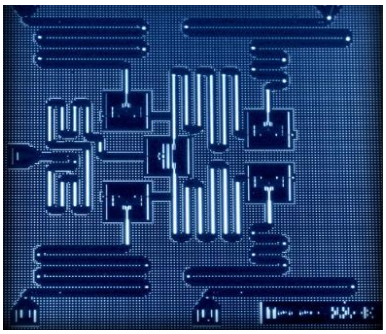


Figura 28. Tarjeta de 5 qbits superconductores de IBM.

Cuando una medición es realizada, el software muestra la calibracion del dispositivo, que incluye algunos parametros como el número de ejecuciones (*shots*) del algoritmo descrito circuitalmente, y los tiempos de relajacion T_1 y T_2, relacionados con la coherencia de los qbits (Figura 28).

Device Calibration

Date Calibration: 2016-05-11 12:05

Fridge Temperature: 0.01423 Kelvin

Q_0	Q_1	Q_2	Q_3	Q_4
T_1: 40.8 μs	T_1: 76.1 μs	T_1: 74.3 μs	T_1: 72 μs	T_1: 65.4 μs
T_2: 51 μs	T_2: 107.3 μs	T_2: 62.9 μs	T_2: 55.3 μs	T_2: 66.7 μs
ϵ_g: 2.8×10^{-3}	ϵ_g: 2.3×10^{-3}	ϵ_g: 2.1×10^{-3}	ϵ_g: 2.3×10^{-3}	ϵ_g: 2.4×10^{-3}
ϵ_r: 5.4×10^{-2}	ϵ_r: 3.4×10^{-2}	ϵ_r: 2.7×10^{-2}	ϵ_r: 9.6×10^{-2}	ϵ_r: 2×10^{-2}
ϵ_g^{02}: 4.56×10^{-2}	ϵ_g^{12}: 3.19×10^{-2}		ϵ_g^{32}: 5.28×10^{-2}	ϵ_g^{42}: 3.23×10^{-2}

Executed on: Oct 31, 2016 10:33:28 AM **Number of shots:** 8192

Results date: Oct 31, 2016 10:33:28 AM

Results from Cache: May 12, 2016 4:29:25 AM

Figura 29. Calibración procesador *IBM Quantum Experience*.

La herramienta *compositor*, permite el diseño y manipulación de circuitos de hasta 5 qbits, mediante el uso de 10 compuertas cuánticas diferentes y dos tipos de mediciones posibles al sistema. Solo es posible efectuar un tipo de medición al sistema, es decir, todas las medidas efectuadas sobre los qbits que se requiera, será del mismo tipo. La figura 30 muestra la interfaz del compositor para diseñar circuitos cuánticos.

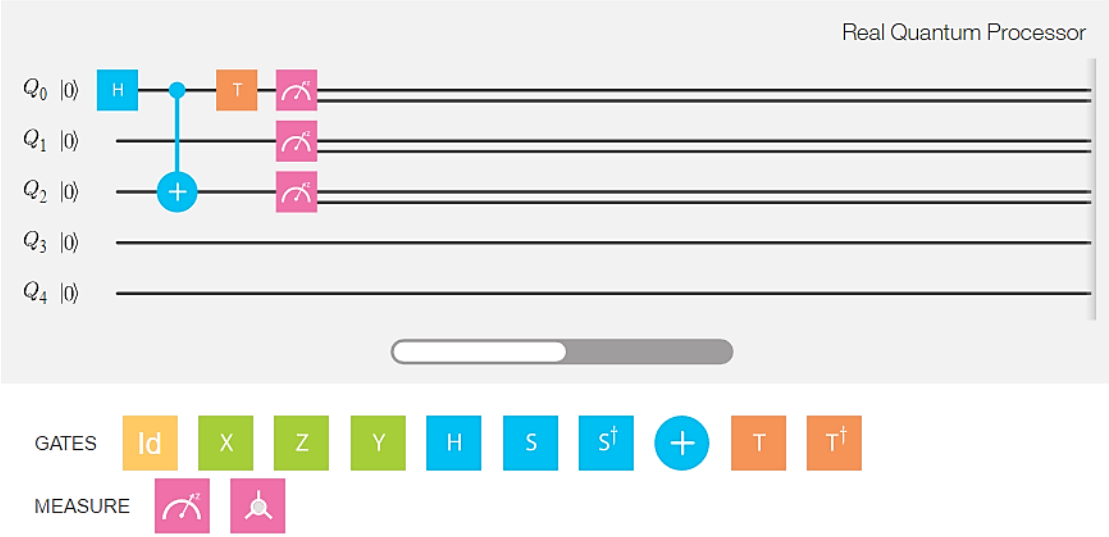


Figura 30. Interfaz del compositor *IBM Quantum Experience*.

Los dos tipos de mediciones posibles son:

- Medición estándar Z: proyección o colapso sobre el eje Z de la esfera de Bloch. El resultado es una gráfica de barras que indica la probabilidad de que el sistema colapse en determinado estado.
- Esfera de Bloch: proyección sobre la esfera de Bloch. Indica el estado final del qbit al ser proyectado en los ejes X, Y y Z. El resultado es un vector sobre la esfera de Bloch.

Se encuentra más información y detalle sobre las compuertas cuánticas y las mediciones que atañen a este trabajo, en el anexo sobre circuitos cuánticos y en [24]. El sistema nunca termina en superposición.

El orden de los qbits es INVERSO al convencional, es decir, Q_0 es el qbit más significativo y Q_4 el menos, como se muestra en la figura 31.

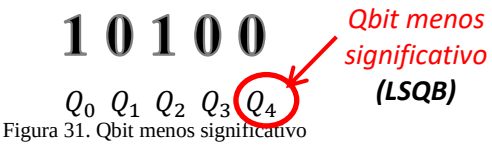


Figura 31. Qbit menos significativo

Adicionalmente, el software registra en lenguaje QASM 2.0, cada transformación que ocurre en el sistema. Por ejemplo, la figura 32 muestra el código que describe el circuito de la figura 30:

```
1 h q[0];
2 cx q[0], q[2];
3 t q[0];
4 measure q[0];
5 measure q[1];
6 measure q[2];
```

Figura 32. Código QASM 2.0.

3.2.2. GOOGLE'S QUANTUM PLAYGROUND:

El *Quantum Playground*, es un experimento de Google que usa WebGL[27] para simular registros de hasta 22 qubits. Cuenta con su propio lenguaje de *scripts*, con depuración y funciones de visualización 3D del estado cuántico. Puede ejecutar algoritmos cuánticos como el de Shor y el de Grover[28], y tiene una variedad de puertas cuánticas incorporadas. Su propósito dentro de este trabajo es el del posibilitar simulaciones con más de 5 qbits.

Es un modelo simulado de un computador cuántico. Tiene un registro con un tamaño ajustable de 6 a 22 qbits. Los usuarios pueden interactuar con el computador cuántico simulado escribiendo scripts usando un lenguaje llamado QScript. Internamente, el registro cuántico es guardado como un vector global del estado del sistema cuántico, en una textura RGB o RGBA punto flotante del tamaño adecuado. Por ejemplo, si un vector de estado tiene 8 qbits, son 256 estados cuánticos, así que la textura que guardará esta información es de dimensiones 16x16 pixeles. Solo se usan los componentes R y G del pixel, para las partes real e imaginaria de los estados cuánticos correspondientemente.

El registro de estado del sistema puede ser visualizado en una gráfica 2D o 3D, en la cual los puntos o barras representan superposiciones de los qbits, mientras el color o altura representa la amplitud y fase de la misma. Una de las propiedades más importantes de las compuertas cuánticas es su carácter reversible, permitiendo ejecuciones de un mismo programa en pasos hacia adelante o hacia atrás del código.

La interfaz de programación y resultados se muestra en la figura 33. Puede dividirse en 4 zonas delimitadas por los recuadros de diferente color y número:

1. Rojo: Resultados en visualización 2D o 3D del vector de estados del sistema cuántico simulado.
2. Azul: Cambio en las variables locales creadas, evolución de sus valores y salidas del sistema.
3. Verde: Botones de compilación, ejecución, pasos hacia adelante y atrás en el código y guardar.
4. Naranja: Programación del sistema cuántico simulado.

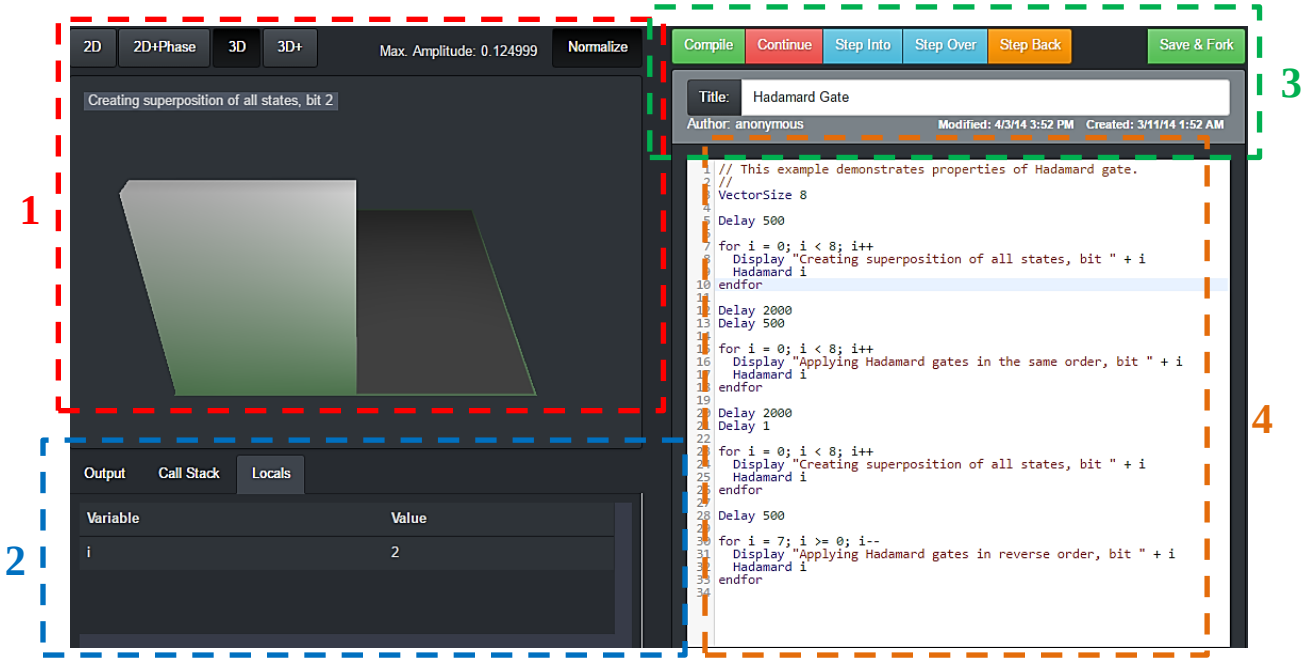


Figura 33. Interfaz gráfica del *Quantum Playground* de Google [25].

[27] Especificación estándar para mostrar gráficos 3D en navegadores Web sin instalar software adicional.
[28] Algoritmo cuántico para la búsqueda de datos dentro listas no ordenadas.

Mayor información sobre el lenguaje Qscript y del funcionamiento interno del *Quantum Playground* se encuentra en [25].

3.2.3. QKD SIMULATOR:

Es una aplicación web desarrollada por Arash Atashpendar, destinada a simular y analizar casi todos los aspectos de distribución de clave cuántica, permitiendo al usuario personalizar los ajustes iniciales y definir nuevas limitaciones en términos de componentes individuales y sub-protocolos en el sistema, por ejemplo, canal cuántico, tamización, estimación de error, reconciliación de información y la amplificación de privacidad [26].

Este software maneja un número máximo de qbits es 600. Va a ser usado dentro del trabajo, para realizar una simulación y análisis completo del protocolo BB84 con la presencia de un espía E. El sistema se prepara con 8 parámetros iniciales:

1. Número de qbits (fotones): entre 500 y 600.
2. Delta de sesgo[29] en la selección de la base de medición (%).
3. Sesgo en la selección del agente E (%).
4. Habilitar estimación de error sesgado: si o no.
5. Tasa de muestreo para la estimación del error (%).
6. Tolerancia al error: Umbral del QBER (%).
7. Habilitar espía E: si o no.
8. Tasa de espionaje (%).

Luego de la simulación, el software realiza un análisis de cada una de las fases del protocolo BB84 con los parámetros iniciales, y resume el valor de las propiedades como se muestra en la tabla 4 [26]:

Property	Value
Initial number of qubits	500
Final key length	40
Estimated error	0.0784
Eavesdropping enabled	1
Eavesdropping rate	0.1
Alice/Bob basis selection bias	0.5
Eve basis selection bias	0.5
Raw key mismatch before error correction	0.0856
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	146
Overall key cost for authentication	256
Key length before error correction	206
Bit error probability	0.0874
Bits leaked during error correction	114
Shannon bound for leakage	89
Security parameter	20

Tabla 4. Ejemplo de resultado de estadísticas y visión general QKD simulator

[29] *Bias* → En este contexto hace referencia a la probabilidad de error en la medición del agente B cuando usa una base incorrecta a la polarización del fotón medido.

3.3. PROTOCOLO DE PRUEBAS

En este apartado, se describen los procedimientos realizados (y su justificación) para obtener las evidencias del cumplimiento tanto del objetivo del proyecto como de los entregables. Se establece que cada entregable es equivalente al cumplimiento de una de las actividades definidas en el flujo de procesos de la figura 25:

- ✓ Verificación del algoritmo de Shor.
- ✓ Comparación del algoritmo de Shor contra algoritmos clásicos para resolver sistema RSA.
- ✓ Verificación del principio cuántico base del BB84.
- ✓ Verificación del fenómeno cuántico del protocolo E91.
- ✓ Comparación en términos de seguridad de los diferentes tipos de criptografía.
- ✓ Identificación e indagación empresarial sobre redes y sistemas criptográfico-cuánticos.

Las dos últimas actividades al igual que la comparación del algoritmo de Shor, no requieren de ningún tipo de protocolo de pruebas. Su resolución se lleva a cabo en el próximo capítulo, análisis de resultados. El resto de las actividades se cumplen en el proceso de diseño y prueba de los circuitos que corresponden y argumentan a: el algoritmo de Shor, el protocolo BB84 y el protocolo E91.

3.3.1. ALGORITMO DE SHOR

El algoritmo de Shor posee un circuito cuántico conocido (Figura 10 dentro del marco teórico). Se hará uso de la plataforma de IBM para ejecutar dos de sus partes: la función U_f de exponenciación modular y la transformada cuántica de Fourier. El circuito completo de la figura 10 no podrá ser ejecutado debido a limitación de 5 qbits del software de IBM. Se ejecutará el oráculo diseñado U_a de la función exponenciación modular como muestra la ecuación 26, para un *a* determinado, al que se le conozca su circuito equivalente [27].

El siguiente paso es realizar una medición a los valores propios del operador unitario U_a descrito por un circuito cuántico, ya que estos poseen información importante sobre el periodo como indica la ecuación 28. Para ello se debe tener una versión de U_7 controlada por un qbit, es decir, una transformación unitaria actuando en un sistema compuesto por un qbit de control y un registro de qbits objetivo. Esta versión controlada de U_a, ejecuta la transformación U_a sobre el registro de qbits solo si el qbit de control se encuentra en el estado $|1>$ (ver anexo sobre circuitos cuánticos).

El registro de qbits está preparado en un estado $]\psi>$, el cual es un vector propio de U_a. Esto significa que ejecutar *U* en el estado $]\psi>$ es igual a:

$$U]\psi>= e^{i\phi} *]\psi> \tag{51}$$

Entonces, la única diferencia entre las dos ramas (Figura 10) de la versión controlada de U_a es el cambio de fase $e^{i\phi}$. El qbit de control recorre desde $a_0|0> + a_1|1>$ hasta $a_0|0> + e^{i\phi} * a_1|1>$, mientras el registro de qbits objetivo permanece en el estado $]\psi>$. Así que la acción de la compuerta U_a controlada, puede ser descrita por una compuerta de cambio de fase actuando en el qbit de control. El circuito cuántico completo no podrá ser simulado o ejecutado con la herramienta de IBM. Sin embargo se establecen los circuitos cuánticos que realizan la estimación de fase [29].

El valor propio $e^{i\phi}$ puede ser medido usando circuitos los circuitos cuánticos para estimación de fase como se ilustra en la figura 34:

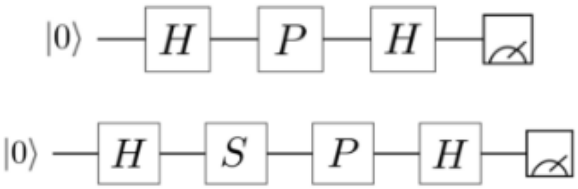


Figura 34. Par para estimación de fase cuántica a qbit control.

Las compuertas P son equivalentes a la transformación unitaria que realiza el desplazamiento de fase $U_{R(\theta)}$ (ver anexo sobre circuitos cuánticos).

La idea es que para extraer información de la fase ϕ, se mida la interferencia entre la rama del operador U_7 controlado que posee el factor de fase $e^{i\phi}$ y la rama que no. Generalmente para amplificar la información estadística en algoritmos cuánticos, se repiten los circuitos varias veces, en este caso para tener la mejor estimación de ϕ.

Después de al menos dos pruebas se podrá hacer un análisis del circuito.

También se usa el simulador de Google para realizar una simulación del algoritmo de Shor completo con valores diferentes del entero que se está factorizando.

El número de qbits del sistema es un valor entre 6 y 22. El número de qbits debe ser par. En este orden de ideas los parámetros están limitados a:

$$2^6 = 64\ estados \rightarrow textura\ de\ 8x8 \tag{52}$$

$$2^{22} = 4\ 194\ 304\ estados \rightarrow textura\ de\ 2048x2048 \tag{53}$$

Según esto, se puede hallar la factorización prima de enteros entre 0 y 4 millones aproximadamente. Se ejecutará el algoritmo para dos rangos de valores con el número de qbits máximo, para generar el espacio de estados más grande posible. Los dos rangos definidos son:

a) 15 – 99. 22 qbits.
b) 100 – 999. 22 qbits.

La variación requiere el cambio dos variables como se muestra en la figura 35.

```
80      if (factor < N) && (factor > 1)
81        Display "<h2>Success: " + factor + " " + N / factor
82        Breakpoint
83      else
84        Print "Unable to determine factors, try again."
85        continue
86      endif
87    endfor
88  endproc
89
90  VectorSize 16
91  FindFactors 15
```

Variable que define el número de qbits

Variable que define el entero de entrada del algoritmo de Shor

Figura 35. Líneas finales de código del algoritmo de Shor de Google.

Los resultados se verán reflejados en los recuadros 1 (rojo) y 2 (azul) de la interfaz gráfica del software mostrada en la figura 33. Si el entero de entrada es un número primo, no se podrá hacer la descomposición. El valor de *n* debe ser un entero no primo que pueda ser escrito de la forma $n = p * q$, donde *p* y *q* son enteros primos y constituyen la solución del problema. Según esto se debe elegir un valor de n que sea **impar y no primo entre los rangos definidos**.

Se realizan variaciones de la variable *FindFactors* en el código del algoritmo de Shor provisto por Google, y se establece aproximadamente que un valor superior a 500, genera errores en la salida de la simulación. Por lo tanto:

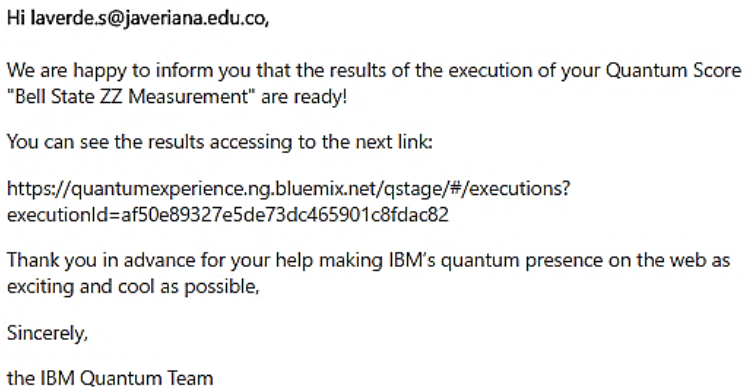
$$FindFactors < 500 \tag{54}$$

El código completo en *Qscript* y usando librería *libquantum* (basada en C++) se encuentra en el anexo sobre el código del algoritmo de Shor.

A partir de este punto se puede realizar la comparación contra algoritmos clásicos, basándose en las bibliografías [29] y [30].

3.3.2. PROTOCOLO BB84

Se hará uso de la plataforma de IBM para validar el principio de incertidumbre de Heisenberg en un procesador cuántico real, mediante el diseño de circuitos que demuestren la incertidumbre provocada por diferentes mediciones sobre varios qbits en la base incorrecta. La incertidumbre generada varía dependiendo del tipo de ejecución efectuada del circuito cuántico. Debido a la naturaleza probabilística de los sistemas cuánticos, si la ejecución es en un procesador real, se debe elegir el número de veces que se desea ejecutar el circuito, a razón de obtener mayor fiabilidad en los resultados. Generalmente hay cola en el uso de los procesadores disponibles. A veces existen resultados almacenados en caché para circuitos equivalentes al que se está ejecutando. Estos pueden ser usados en vez de esperar la finalización de la ejecución nueva. Una vez terminada la ejecución en el procesador real, se recibe un mail de confirmación como se muestra en la figura 36.



Hi laverde.s@javeriana.edu.co,

We are happy to inform you that the results of the execution of your Quantum Score "Bell State ZZ Measurement" are ready!

You can see the results accessing to the next link:

https://quantumexperience.ng.bluemix.net/qstage/#/executions?executionId=af50e89327e5de73dc465901c8fdac82

Thank you in advance for your help making IBM's quantum presence on the web as exciting and cool as possible,

Sincerely,

the IBM Quantum Team

Figura 36. Confirmación de ejecución exitosa IBM.

El resultado de la medición será de tipo probabilístico y podrá ser representado con un diagrama de barras cuya amplitud representa la probabilidad de que la medición (colapso de la función de onda probabilística) resulte en determinado estado u otro. A modo de ejemplo se presenta un resultado para cada tipo de ejecución del circuito cuántico de la figura 37:

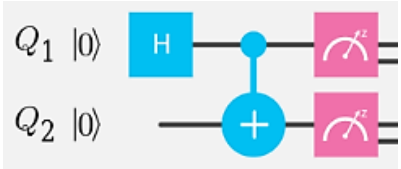


Figura 37. Circuito cuántico, mediciones Z-Z.

Idealmente la distribución probabilística es de 0,5 para los códigos 00 y 11, y de 0,0 para 01 y 10, como se muestra en la figura 38.

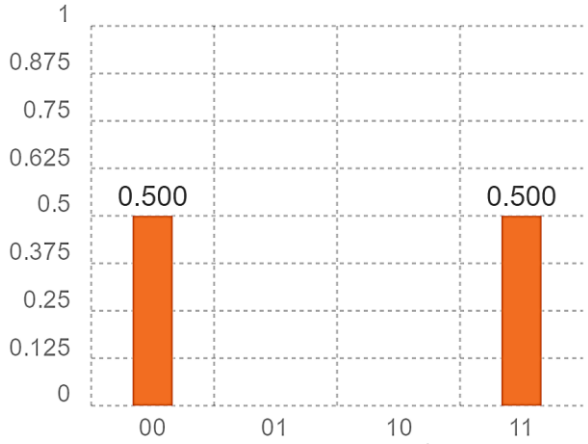


Figura 38. Simulacion con procesador cuántico ideal.

Las figuras 39 y 40 muestran resultados en barras, de simulación con condiciones realistas y de una ejecución en un procesador cuántico real respectivamente.

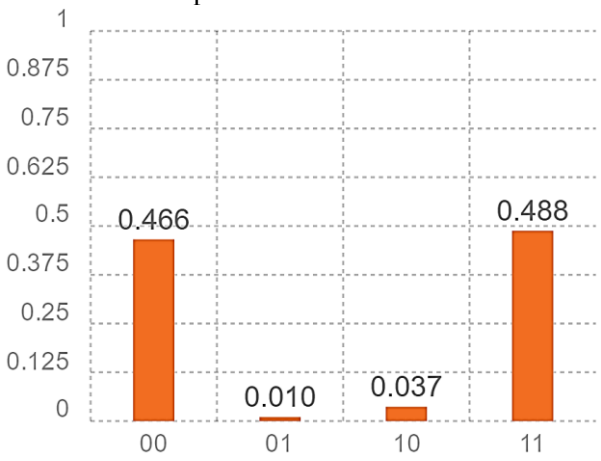


Figura 39. Simulación con condiciones realistas

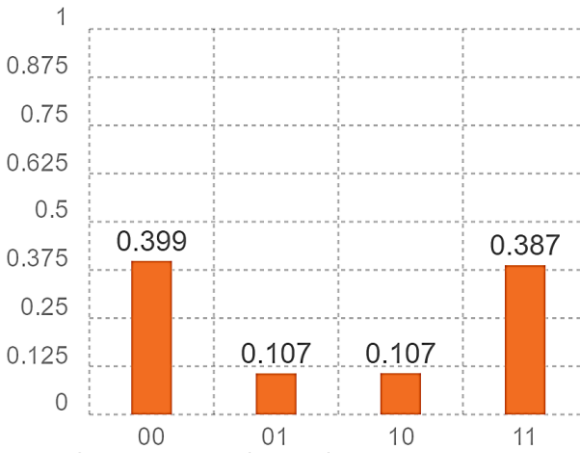


Figura 40. Ejecución en procesador cuántico. Número de iteraciones del circuito = 8192

Se trabaja con los resultados de la ejecución en el procesador cuántico real. Las fuentes de error en la ejecución de un algoritmo en un procesador cuántico real, son varias e inevitables, y sus efectos deben considerarse para un análisis más completo. Ver anexo sobre circuitos cuánticos.

Se usa el simulador online de QKD para probar diferentes valores de los parámetros de entrada, y analizar los resultados. La interfaz que permite la variación de estos parámetros, se muestra en la figura 38.

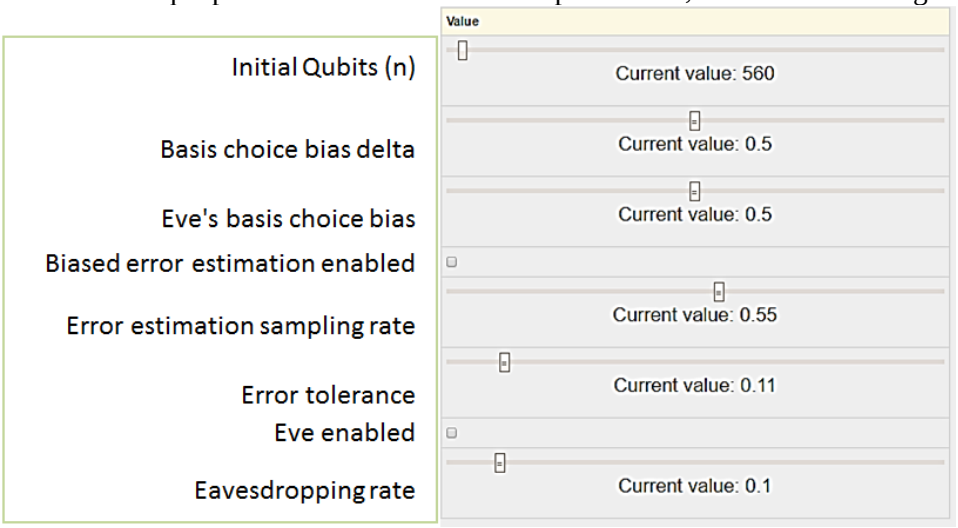


Figura 41. Interfaz variación parámetros iniciales *QKD simulator*.

3.3.3. PROTOCOLO E91

Se hará uso de la plataforma de IBM para demostrar que las correlaciones cuánticas violan la desigualdad CHSH, y por lo tanto se rigen por principios distintos a los de *realismo* y *localidad*, los cuales gobiernan a las correlaciones clásicas. Para ellos se efectuarán distintas mediciones a uno de los estados de Bell:

$$|\psi>_{A\otimes B} = |\psi>_A \otimes |\psi>_B = \frac{1}{\sqrt{2}}\,(|0>_A |0>_B + |1>_A |1>_B) \tag{43}$$

Las mediciones deberán ser ortogonales entre sí. El estado puede ser simulado y ejecutado por la plataforma de IBM, mediante compuertas cuánticas que modifican el estado de los qbits, como lo son la CNOT cuántica y la compuerta *Hadamard*. Ver anexos sobre circuitos cuánticos y [29].

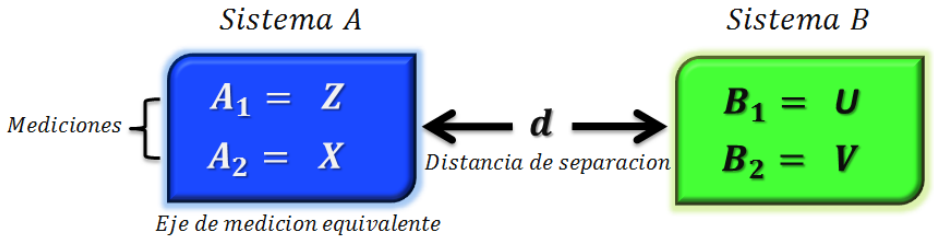


Figura 42. Mediciones elegidas para sistema entrelazado.

Se definen Z y X como los ejes respectivos en esfera de Bloch, y

$$U = \frac{1}{\sqrt{2}}\,(Z + X) \tag{44}$$

$$V = \frac{1}{\sqrt{2}}\,(Z - X) \tag{45}$$

Se debe corroborar que las mediciones elegidas sean ortogonales entre sí. Es posible hacer una verificación matemática pero la representación en la esfera de Bloch es suficiente para comprobarlo. A

partir de ahí, se puede determinar el valor absoluto de la correlación C para dos sistema A y B entrelazados cuánticamente, según las ecuaciones 32 y 34 del marco teórico.

Si el valor de la correlación es menor a 2, la correlación es clásica y se rige por los principios clásicos definidos, pero si no, es una violación a la desigualdad CHSH y se demuestra el fenómeno físico cuántico que hace posible la funcionalidad de protocolos basados en el efecto EPR.

3.4. RESULTADOS

3.4.1. VERIFICACIÓN DEL ALGORITMO DE SHOR

El circuito cuántico usado que ejecuta la transformación unitaria de multiplicación modular U_7 :

$$x \rightarrow 7 * x \; mod \; 15 \tag{46}$$

es el mostrado en la figura 42, donde *x* corresponde a la inicialización de los qbits para calcular el módulo 15 de 7*x*. El circuito está compuesto solo por compuertas NOT y compuertas SWAP. Ver anexo sobre circuitos cuánticos.

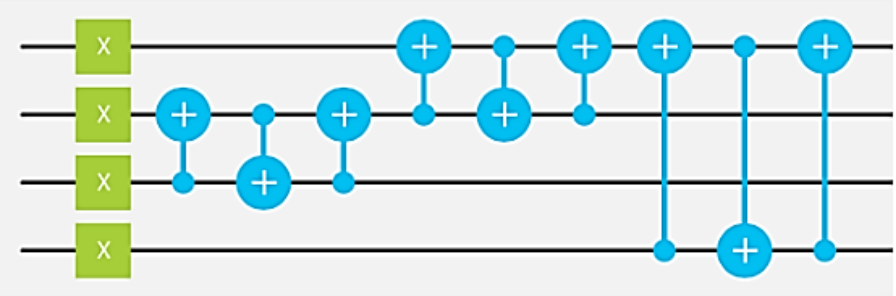


Figura 43. Circuito de multiplicación modular *7x mod 15*[30]

Se realizan las simulaciones de la función multiplicación modular $13 \rightarrow 7 * 13 \; mod \; 15$ y la función multiplicación modular $6 \rightarrow 7 * 6 \; mod \; 15$ siendo el qbit 4, el menos significativo. Los circuitos son los mostrados en las figuras 43 y 44 respectivamente.

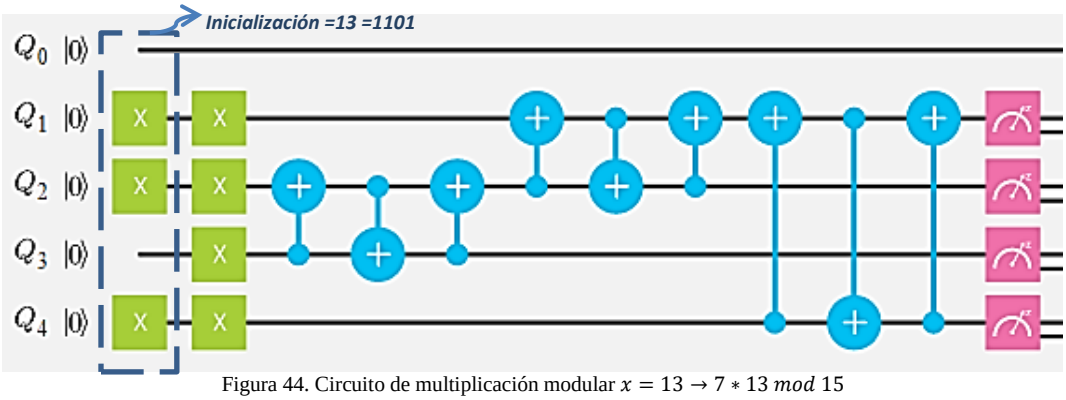


Figura 44. Circuito de multiplicación modular $x = 13 \rightarrow 7 * 13 \; mod \; 15$

[30]https://quantumexperience.ng.bluemix.net/qstage/#/tutorial?sectionId=8443c4f713521c10b1a56a533958286b&pageIndex=5

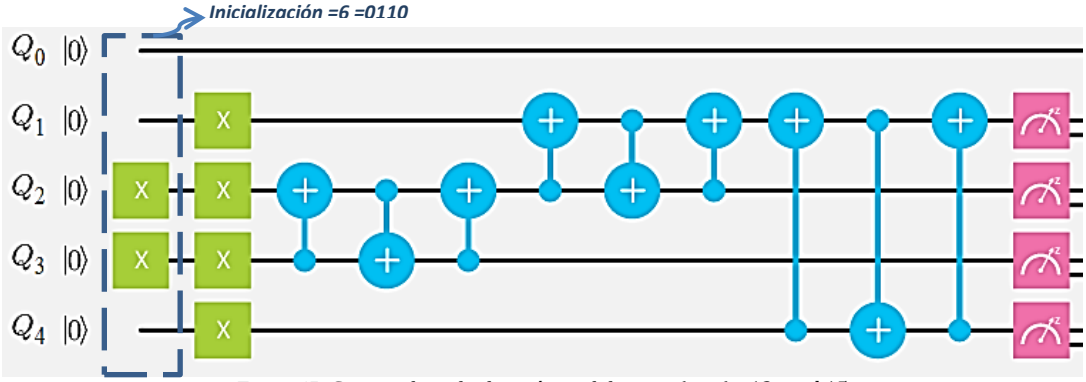


Figura 45. Circuito de multiplicación modular $x = 6 \rightarrow 6 * 13\ mod\ 15$

Los resultados para la medición realizada sobre el sistema se puede observar en la figura 45:

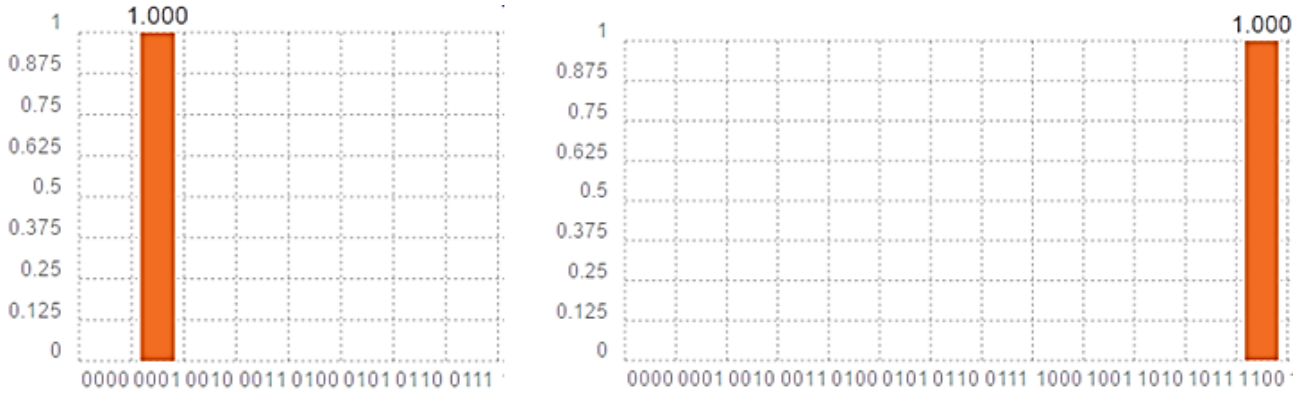


Figura 46. Resultados en barras probabilísticas de circuitos de multiplicación modular.

Se comprueba que los valores deben resultar en:

$$13 \rightarrow 7 * 13\ mod\ 15 = 1 \rightarrow 0001 \tag{47}$$

debido a que:

$$7 * 13 = 91 \quad y \quad 15 * 6 = 90 \quad entonces\ 91\ mod\ 15 \rightarrow 0001 \tag{48}$$

y en:

$$6 \rightarrow 7 * 6\ mod\ 15 = 12 \rightarrow 1100 \tag{49}$$

debido a que:

$$7 * 6 = 42 \quad y \quad 15 * 2 = 30 \quad entonces\ 42\ mod\ 15 \rightarrow 1100 \tag{50}$$

Como las ejecuciones fueron realizadas en el modo simulación (debido a la topología del procesador). Los resultados dan con probabilidad del 100%.

Los circuitos equivalentes para la estimación de la fase usando las compuertas cuánticas del compositor del *IBM Quantum Experience* se ven en la figura 47. Ver título **tecnología utilizada** y anexo sobre circuitos cuánticos.

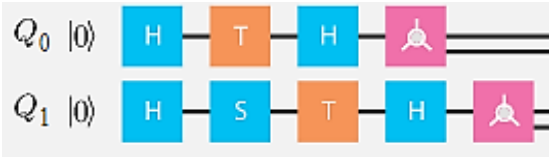


Figura 47. Circuitos para estimación de fase compuerta Toffoli.

La representación en la esfera de Bloch de las dos estimaciones se muestra en la figura 48:

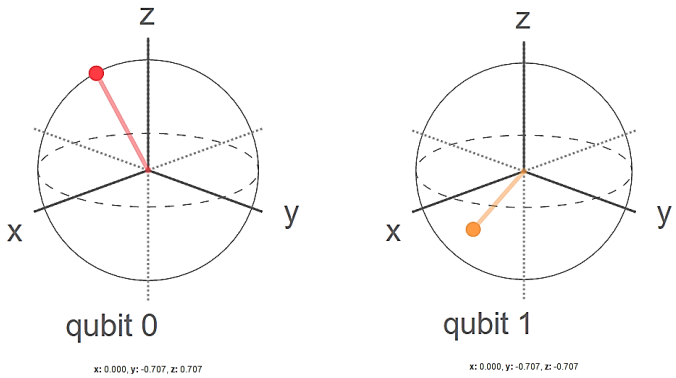


Figura 48. Grafico 4. Esfera de *Bloch* resultado de circuito 2. *Qbit 0 (0,-0,707, 0,707), Qbit 1(0, -0, 707,-0,707)*

En las figuras 49 y 50, se muestran los resultados de la ejecución del algoritmo de Shor usando el software de Google, para dos valores de *n* diferentes usando los rangos de enteros no primos definidos en el protocolo de pruebas.

Los primeros 25 números primos son {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}. Este grupo es suficiente para determinar los valores de *n* con los que se ejecutará el algoritmo de Shor. Las ejecuciones se realizan con las variables *VectorSize* = 22 *y FindFactors* = *n*

a) $p * q = 3 * 27 = 81$

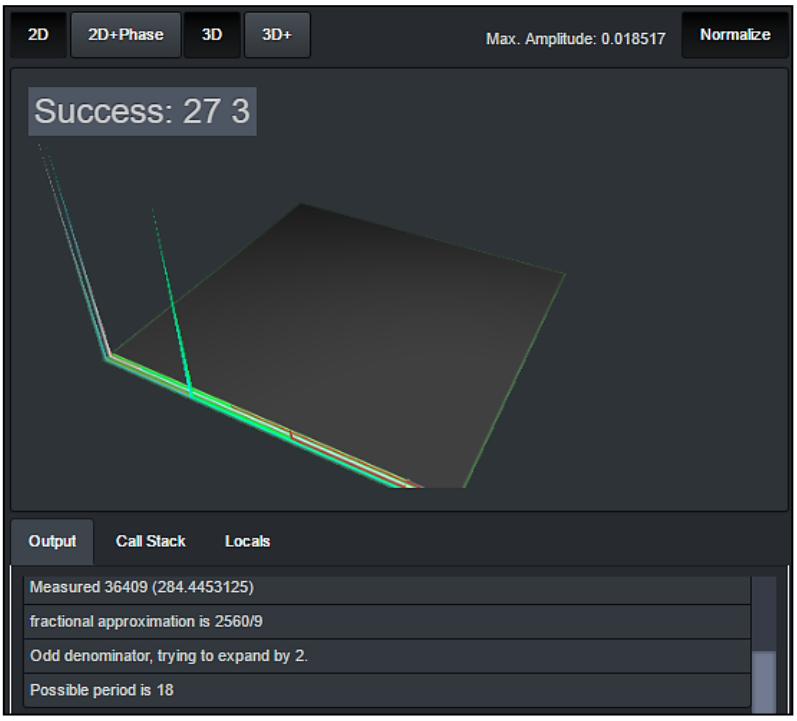


Figura 49. Algoritmo de Shor de Google. *FindFactors* = 81, *VectorSize* = 22.

b) $p * q = 19 * 23 = 437$

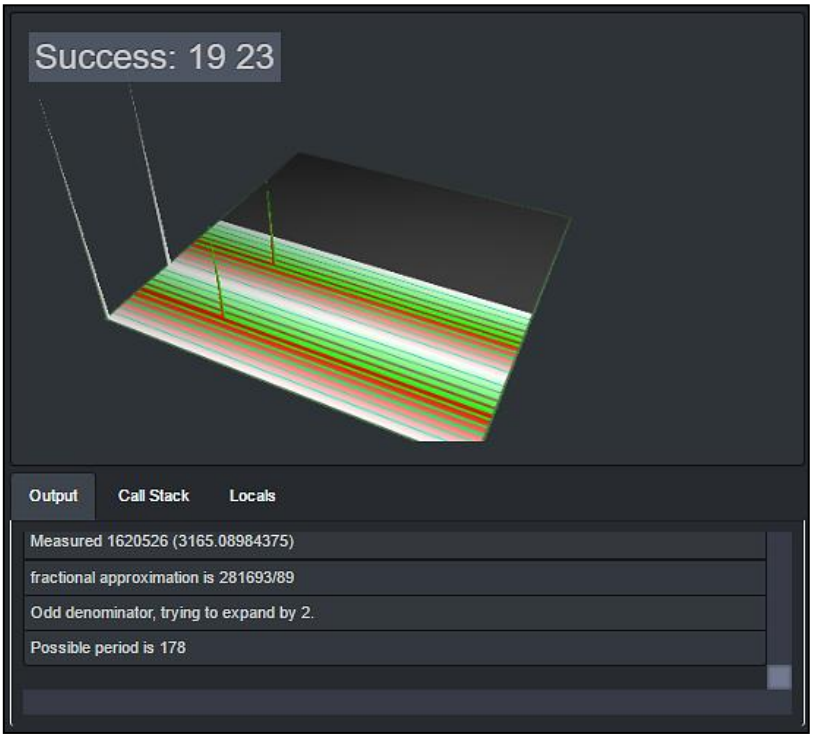


Figura 50. Algoritmo de Shor de Google. *FindFactors* = 437, *VectorSize* = 22.

3.4.2. VERIFICACIÓN DEL PROTOCOLO BB84

Se recuerda que la característica más importante de la distribución de claves cuánticas entre dos usuarios remotos, es que cualquier intento de espionaje dentro del canal, siempre se introduce inmediatamente perturbaciones en la señal que pueden ser detectadas por los usuarios involucrados. Para comprobar esto, se puede usar la plataforma de IBM, para ejecutar en un procesador real el resultado probabilístico de medir un fotón con un filtro polarizador determinado.

Los circuitos mostrados en la figura 51 son usados para representar los ejes de medición correspondientes a pasar el fotón por polarizadores de tipo:

- Lineal rectilíneo (0º/90º).
- Lineal diagonal (45º/135º).
- Circular o esférico.

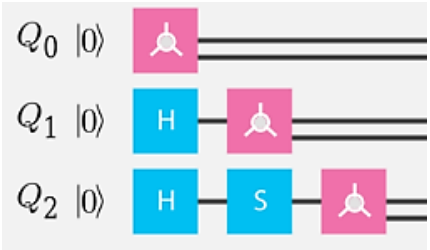


Figura 51. Circuitos equivalentes a 3 tipos de polarizadores distintos.

La figura 52 ilustra los ejes correspondientes en la esfera de Bloch.

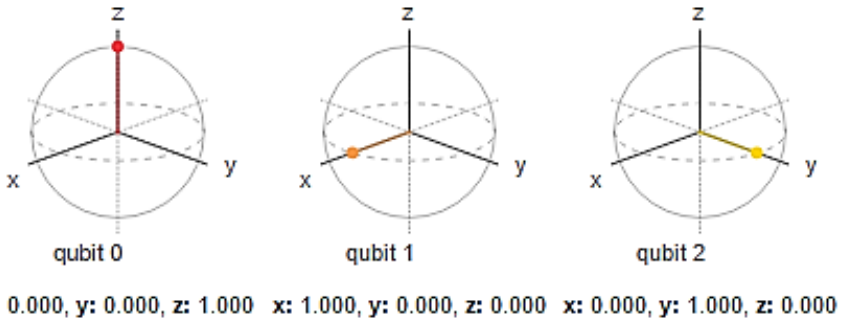


Figura 52. Mediciones equivalentes en la esfera de Bloch.

El eje Z hace las veces del resultado de una medición sobre el qbit al pasar por un filtro polarizador de tipo rectilínea, y los ejes X, Y, filtros polarizadores de tipo diagonal y circular o elíptico respectivamente. La idea es corroborar que un fotón, representado por un qbit, tiene un 50% de probabilidades de ser medido como un 1 o un 0, si la medición es efectuada con un filtro polarizador del tipo incorrecto. La esfera de Bloch sirve para ilustrar la correspondencia de los ejes, con el tipo de polarizador utilizado. Pero los gráficos con barras ilustran la distribución probabilística de los resultados de las mediciones.

Se realizarán 4 mediciones de los 3 tipos a qbits que se encuentran en estados diferentes dentro de la base lineal rectilínea, es decir 0º y 90º con respecto al eje Z. Se recuerda que el orden de los qbits dentro del código del procesador y sus resultados es el mostrado en la figura 31, contrario a la lógica con bits convencional.

El siguiente circuito cuántico de la figura 53 ilustra los estados y mediciones realizadas en los qbits

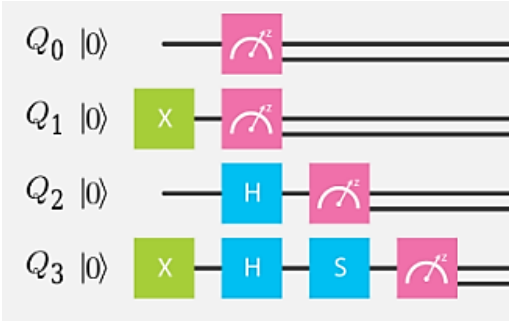


Figura 53. Configuración de prueba de incertidumbre.

Y el resultado en barras se muestra en la figura 54:

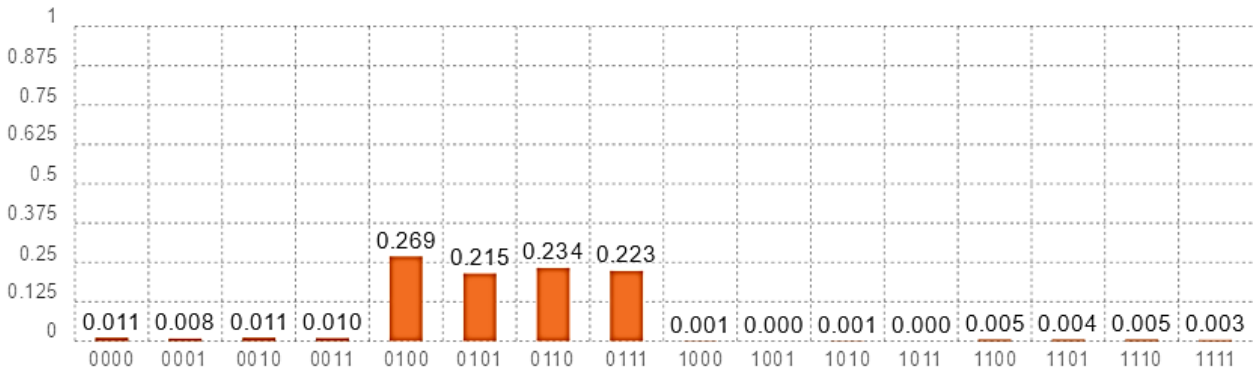


Figura 54. Resultado de ejecución circuito prueba. # *Shots* = 8192.

A modo de ejemplo para evaluar parámetros de seguridad en la clave generada por el este protocolo cuántico, se utiliza el *QKD simulator* para simular el comportamiento de generación de la clave y su destilación, frente a la intervención de un espía en el canal. En la figura 55 se muestran la configuración inicial y la tabla de resultados que entrega el software.

Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
580	0.5	0.5	1	0.25	0.3	1	0.2

Property	Value
Initial number of qubits	580
Final key length	15
Estimated error	0.1778
Eavesdropping enabled	1
Eavesdropping rate	0.25
Alice/Bob basis selection bias	0.5
Eve basis selection bias	0.5
Raw key mismatch before error correction	To be added...
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	182
Overall key cost for authentication	256
Key length before error correction	217
Bit error probability	0.1152
Bits leaked during error correction	150
Shannon bound for leakage	112
Security parameter	20

Figura 55. Resultados de ejecución del QKD Simulator.

El proceso que realiza el simulador es similar al descrito en el marco teórico. Cada parte será considerada en el análisis de resultados.

3.4.3. VERIFICACIÓN DEL PROTOCOLO E91

El valor esperado de las correlaciones está determinado por la ecuación (34). Idealmente, apoyándose en [29] sus valores calculados son:

$$\langle ZU \rangle = {}^{1}/_{\sqrt{2}} \tag{51}$$

$$\langle ZV \rangle = {}^{1}/_{\sqrt{2}} \tag{52}$$

$$\langle XU \rangle = {}^{1}/_{\sqrt{2}} \tag{53}$$

$$\langle XV \rangle = -{}^{1}/_{\sqrt{2}} \tag{54}$$

Ahora se aplica la ecuación (32) para determinar el valor absoluto de la correlación C resultante es:

$$|C| = |\langle ZU\rangle + \langle ZV\rangle + \langle XU\rangle - \langle XV\rangle| = \left|\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \left(-\frac{1}{\sqrt{2}}\right)\right| = 2\sqrt{2} = \mathbf{2,828 \pm 0,004} \quad (55)$$

Esto claramente es una violación a la desigualdad de CHSH y por ende una violación a los principios de realismo y localidad.

Para realizar una comprobación experimental, Se usa la plataforma de IBM para ejecutar en un procesador real el resultado probabilístico de medir un sistema de estados entrelazados. Se precisa de un circuito cuántico que produzca el entrelazamiento entre dos qbits, y una representación de cada una de los 4 tipos de mediciones a ejecutar. El estado de Bell entrelazado y las mediciones a efectuar a cada qbit se ven en la figura 56.

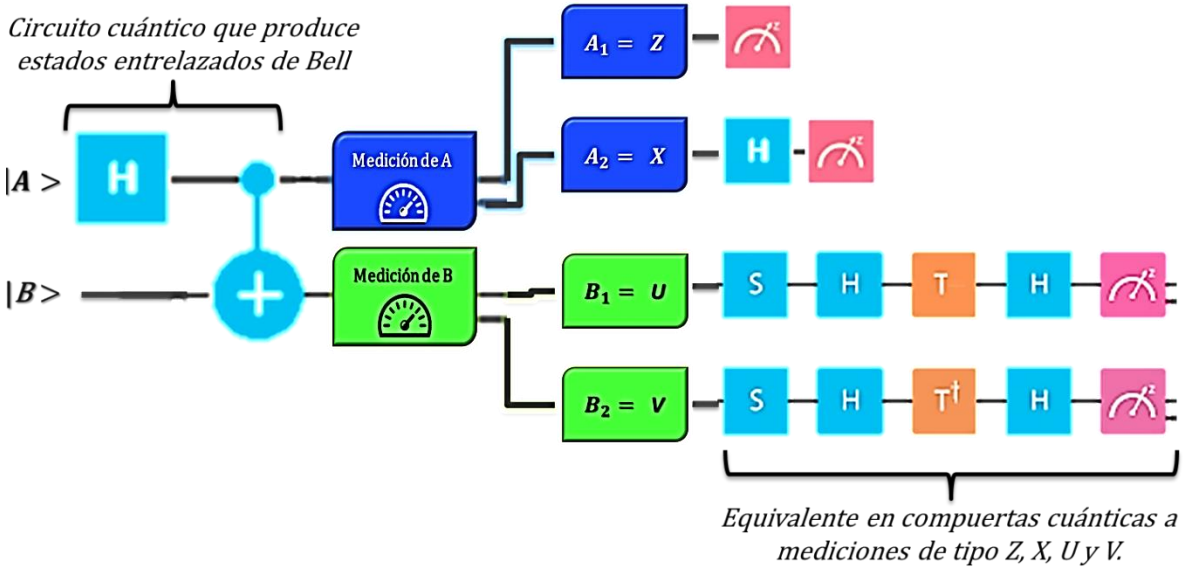


Figura 56. Esquema del circuito cuántico para probar la desigualdad CHSH.

Como se observa se necesita mediciones tipo ZU, ZV, XU, y XV al circuito que entrelaza los qbits 1 y 2 en el estado de Bell.

El circuito cuántico correspondiente para generar tal representación de las bases se ve mejor en la figura 57:

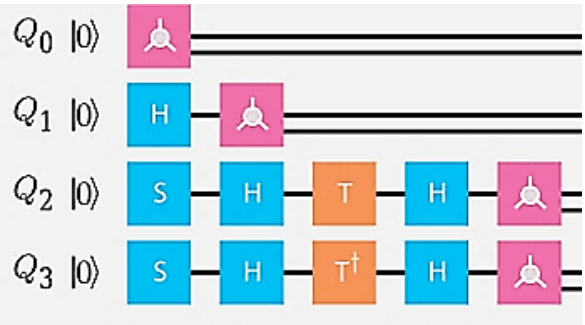


Figura 57. ZXUV en un circuito cuántico.

Donde cada Qbit (Q_0, Q_1, Q_2, Q_3) corresponde a las 4 mediciones a efectuar respectivamente (Z, X, U, V) en los sistemas.

En la figura 58 se observa el eje correspondiente a cada medición (Z, X, U, V) en la esfera de Bloch y su vista superior:

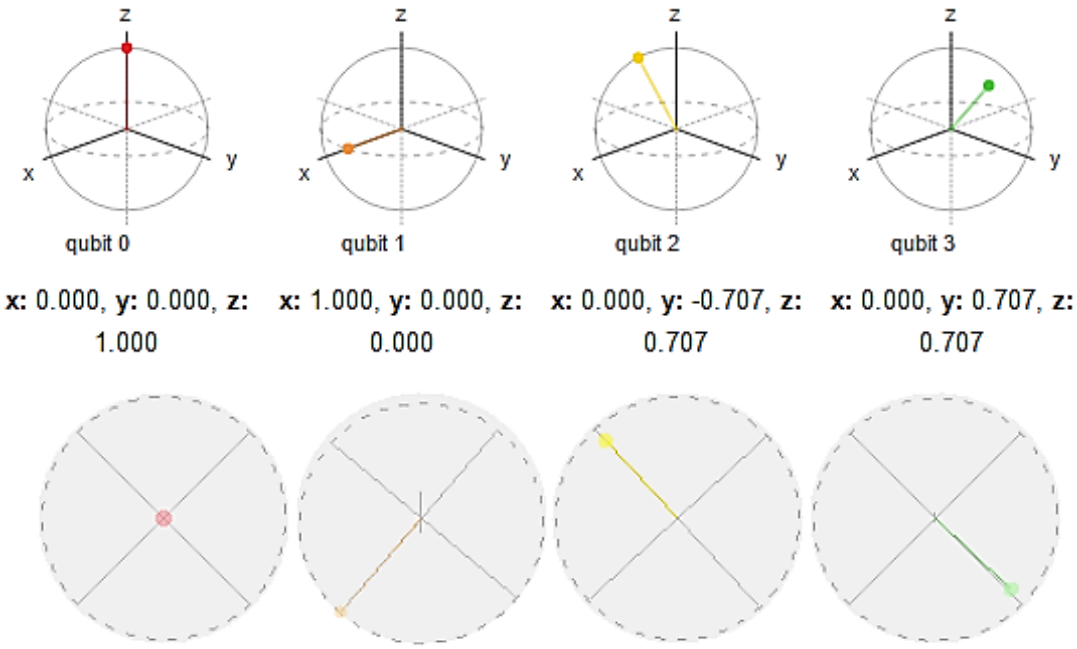


Figura 58. ZXUV en la esfera de Bloch.

Se observa que las bases conforman un grupo ortogonal entre ellas.

El resultado de las mediciones se puede observar en las figuras de la 59 a la 66:

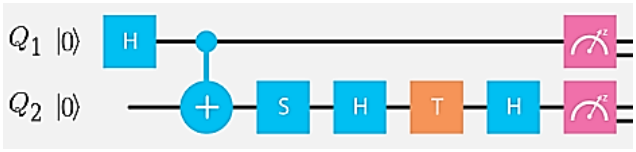


Figura 59. Medición Z al sistema 1 / medición U al sistema 2.

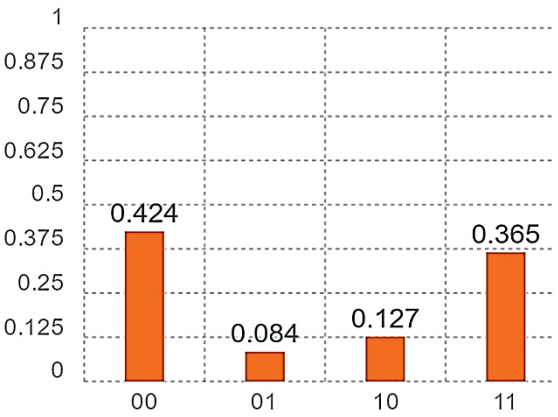


Figura 60. Resultados ZU. 8192 ejecuciones.

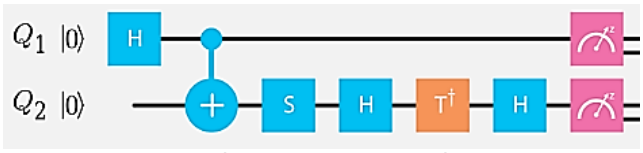


Figura 61. Medición Z al sistema 1 / medición V al sistema 2.

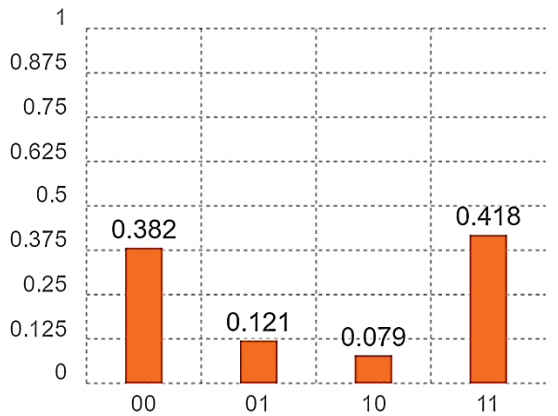


Figura 62. Resultados ZV. 8192 ejecuciones.

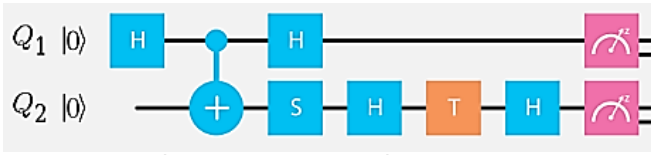


Figura 63. Medición X al sistema 1 / medición U al sistema 2.

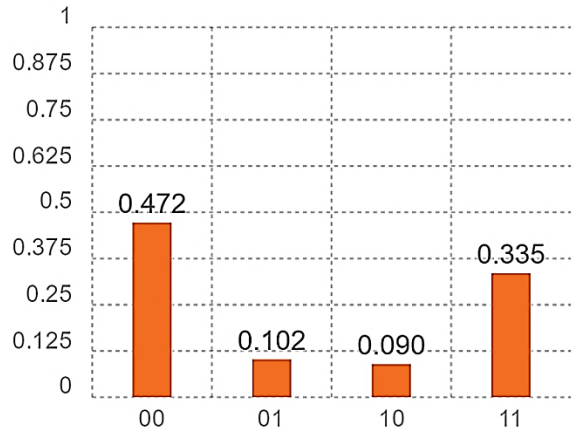


Figura 64. Resultados XU. 8192 ejecuciones.

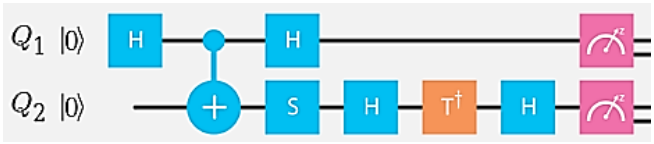


Figura 65 Medición X al sistema 1 / medición V al sistema 2.

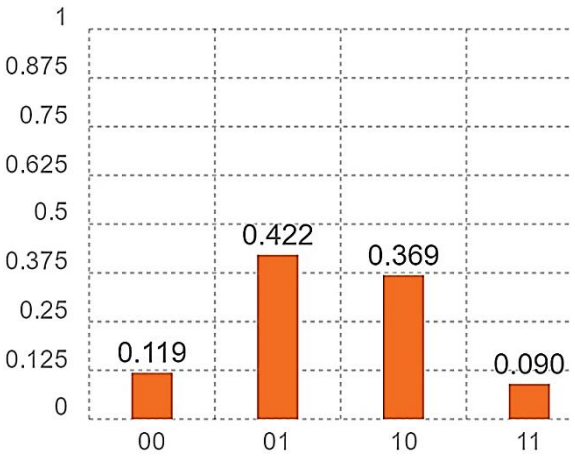


Figura 66. Resultados XV. 8192 ejecuciones.

En el análisis de resultados, se consignan los datos en la tabla 6, para establecer los valores de correlación resultantes y compararlos con los teóricos calculados y con implementaciones similares.

5. ANÁLISIS DE RESULTADOS

5.1. SUPERIORIDAD DEL ALGORITMO DE SHOR

Con las simulaciones se observó una posible implementación de la exponenciación modular en un circuito reversible, y de las transformaciones unitarias correspondientes a la estimación de la fase cuántica. Uno de los aspectos más importantes de la implementación del algoritmo cuántico es que dos ramas de una sentencia condicional pueden ser ejecutadas al mismo tiempo.

Debido a la naturaleza del cómputo cuántico, la mayoría de sus algoritmos deben ser ejecutados más de una vez, para aumentar la exactitud en la respuesta. Sin embargo, la probabilidad de que se encuentre una solución al problema de factorización de enteros, del que se aprovecha el esquema RSA, con el algoritmo de Shor es:

$$P(solucion) = 1 - \left(\frac{1}{2}\right)^{T} \tag{56}$$

Con T = número de ejecuciones del algoritmo.

Debido a esto es muy poco probable que no se encuentre una solución en pocas ejecuciones del algoritmo. En la teoría de la complejidad computacional, se suele realizar la distinción entre algoritmos de Tiempo polinómico y algoritmos de tiempo exponencial cuando se trata de caracterizar a los algoritmos como "suficientemente eficiente" y "muy ineficiente" respectivamente.

Un algoritmo de tiempo polinomial se define como aquel con función de complejidad temporal en O (p(n)) para alguna función polinómica *p*, donde *n* denota el tamaño de la entrada. Cualquier algoritmo cuya función de complejidad temporal no pueda ser acotada de esta manera, se denomina algoritmo de tiempo exponencial.

La mayoría de los algoritmos de tiempo exponencial son simples variaciones de una búsqueda exhaustiva, mientras que los algoritmos de tiempo polinomial, usualmente se obtienen mediante un análisis más profundo de la estructura del problema. En la teoría de la complejidad computacional, existe el consenso de que un problema no está "bien resuelto" hasta que se conozca un algoritmo de tiempo polinomial que lo resuelva. Por tanto, nos referiremos a un problema como intratable, si es tan difícil que no existe algoritmo de tiempo polinomial capaz de resolverlo.

El algoritmo de la criba general de campo de números, es actualmente el algoritmo de factorización más rápido conocido. Su complejidad, dado un número de tamaño m, según [30] y [31] es

$$Orden\ Complejidad\ Computacional\ clasico = \boldsymbol{O}(\boldsymbol{e}^{(c+\boldsymbol{O}(1))*\boldsymbol{m}^{1/3}*(\log \boldsymbol{m})^{2/3}}) \tag{57}$$

Siendo c una constante que depende de la variante del algoritmo.

El orden de complejidad computacional de las compuertas Hadamard es de $O(\log(N))$

El orden de complejidad computacional del operador QFT es de $O(log^2(N))$

El orden de complejidad computacional del oráculo U_f es de $O(log^4(N))$

El orden total será el peor caso entre ellos, así que:

$$Orden\ Complejidad\ Computacional\ Shor = \boldsymbol{O(log^4(N))} \quad (58)$$

Lo cual es extremadamente rápido considerando la probabilidad de éxito del algoritmo.

La figura 67 y cuadro muestran una comparación en número de operaciones y tiempo de solución del algoritmo de Shor vs el algoritmo de la criba general de campo de números resolviendo el problema de encontrar los factores primos de un entero de *d* dígitos:

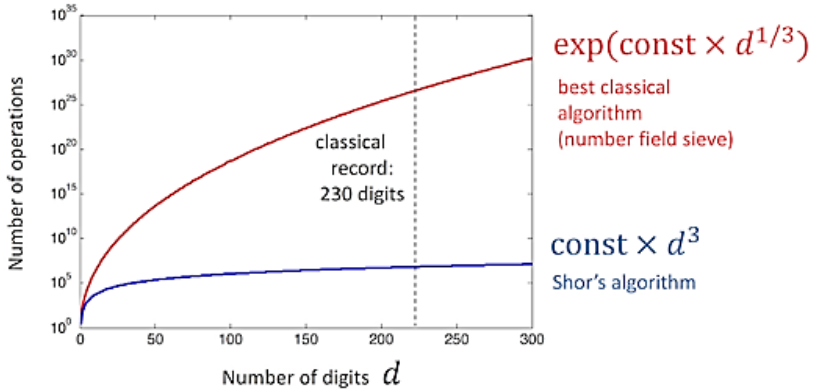


Figura 67. Algoritmo de Shor vs. Mejor algoritmo clásico [29].

En la tabla 5, se compara el tiempo que le toma a un algoritmo clásico contra el tiempo que le toma al algoritmo de Shor, factorizando al mismo entero de longitudes diferentes.

Longitud del Número a factorizar	Tiempo de factorizacion de algoritmo clasico	Tiempo de factorizacion de algoritmo de Shor
512	4 dias	34 segundos
1024	100 mil años	4,5 minutos
2048	100 mil billones de años	36 minutos
4096	100 mil billones de cuadtrillones de años	4,8 horas
8192	∞	1 dia y medio

Tabla 5. Tiempos de factorización según longitud del entero: clásico vs cuántico [30] [32].

Es evidente que para enteros de 1024 dígitos y superiores, el tiempo de factorización que le lleva a un algoritmo clásico, hace absurda la tarea. Es por ello que se considera seguro al esquema RSA. Sin embargo, un procesador capaz de ejecutar el algoritmo de Shor, factorizaría al mismo entero en no más de 5 minutos. Los algoritmos clásicos para solucionar el esquema de criptografía pública RSA, que protege grandes cantidades de nuestra información más sensible, presentan una solución de tipo exponencial. Es por ello que es un sistema muy usado y considerado seguro. Basta con que exista el primer computador cuántico que pueda ejecutar el algoritmo de Shor para enteros más grandes, para que este sistema pueda ser quebrado fácilmente, y con esto la seguridad de muchas redes de comunicación.

5.2. ANÁLISIS DE LA VERIFICACIÓN DEL PROTOCOLO BB84

Los resultados de la figura 54 son coherentes con lo esperado. En los qbits Q_0 y Q_1 se realizan mediciones de tipo lineal rectilínea, por lo que la probabilidad de que el estado del qbit colapse en uno de los estado de la base es del 100% y del 0% en el otro estado. En este caso, el estado antes de la medición de Q_0 es de 0º, lo que equivale a un 0 en el eje Z; y el estado antes de la medición de Q_1 es de 90º, lo que equivale a un 1 en el eje Z. Es por esto que se observa en la barras, que la distribución probabilística es de casi 0% en los códigos en los que Q_0 sea 1 y Q_1 sea 0. En los qbits Q_2 *y* Q_3, las mediciones realizadas son de tipo lineal diagonal y circular o esférico respectivamente, lo que generara incertidumbre en el colapso sobre las bases del eje Z (lineal rectilínea), es decir en el 50% de las 8192 ejecuciones del algoritmo del circuito cuántico, Q_2 colapsará en un 0_z, y el 50% en 1_z. Como el Q_3, también es medido en una base que no corresponde (filtro diferente al lineal rectilíneo), deberá presentar una incertidumbre similar en su estado resultante. La probabilidad total de cada código puede ser entendida como el producto de las probabilidades que experimenta cada qbit de colapsar en ese estado (0_z *o* 1_z) al ser medido. Por eso hay un 25% de probabilidad de colapsar en un código en el que

$$Q_0 = 0 \tag{59}$$

$$Q_1 = 1 \tag{60}$$

$$Q_2 = 1\ (50\%\ de\ las\ veces), 0\ (50\%\ de\ las\ veces) \tag{61}$$

$$Q_3 = 1\ (50\%\ de\ las\ veces), 0\ (50\%\ de\ las\ veces) \tag{62}$$

Los dos usuarios pueden detectar la presencia de espías dado que estos introducirán perturbaciones en los qbits que se envían de A a B. Para ello se denomina la discrepancia *d* como la probabilidad de que un qbit en la clave de la cadena resultante de B, no coincida con la que registra A. La fidelidad en la clave de B es entonces

$$1 - d: fidelidad\ en\ la\ clave \tag{63}$$

La figura 68 ilustra la incertidumbre generada por medir un fotón en el estado y base $|\psi_0 >= |0>$, cuando se miden con las bases rectilínea o diagonal (R o D).

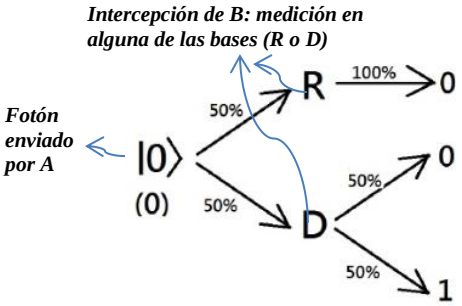


Figura 68. Incertidumbre en la selección de R o D.

La cantidad de aciertos en la cadena del espía midiendo la transmisión del mismo un fotón enviado, siguiendo la estrategia de interceptar y reenviar, es:

$$Aciertos\ en\ la\ cadena\ del\ espia = \frac{1}{2} + \frac{1}{2} * \frac{1}{2} = \mathbf{75}\% \tag{64}$$

Lo cual introduce una discrepancia de 25% en la cadena de la clave de Bob. De modo que compartiendo por un canal público el 50% de la clave obtenida, o con técnicas de comparación de paridad, se decide si hay un espía y se aborta o no la comunicación.

Se hace un análisis de los resultados de la figura 55 del proceso del protocolo BB84 que ejecuta el simulador como se muestra en [26]:

Fase 1: Transmisión Cuántica:

A prepara una secuencia de 580 qubits y los envía a B sobre el canal cuántico. A escoge al azar una base para cada qubit: polarización rectilínea (grados horizontales/0 y grados verticales/90) o una polarización diagonal (+45 grados y-45 grados cambiados). Luego traza un mapa de horizontal y vertical con el qubit y declara |0> y |1> (sobre el eje Z de la esfera de Bloch), y +45 grados y-45 grados cambiados con los estados | +> y | -> respectivamente (eje X de la esfera de Bloch). Detalles:

- A envió 580 qbits a B con una tendencia de selección de base de 0.5.
- E escucha disimuladamente sobre el canal cuántico en una tasa de 0.25 y con una tendencia de selección de base de 0.5. E intercepta los qubits, al azar los mide en una de las dos bases mencionadas y así destruye los originales, y luego envía una nueva hornada de qubits correspondiente a sus medidas y opciones de base a B. Ya que E puede escoger la base correcta sólo el 50 % de las veces en promedio, al menos un 1/4 de sus qbits son diferentes a los que registra A.

Fase 2.1: Destilación:

B anuncia sobre un canal público clásico los qubits que él ha logrado medir satisfactoriamente. Luego A y B revelan las bases que ellos usaron. Siempre que las bases resulten emparejar - aproximadamente el 50 % las veces en promedio - ellos ambos añaden e qbit correspondiente a su clave personal. En ausencia del ruido de canal, las dos claves deberían ser idénticas a no ser que hubiese espionaje.

Fase 2.2: La Autenticación de la destilación- *Registro de desplazamiento de realimentación Lineal (LFSR) Hashing Universal*:

A y B autentican su intercambio de mensajes con la información de bases que eligieron para enviar y medir la cadena de fotones, utilizando el esquema LFSR universal hashing y una clave mutuamente pre-compartida secreta para la autenticación. 3 mensajes son autenticados en proceso de destilación. Detalles:

- B informa a A sobre los qubits que logró medir satisfactoriamente y añade una etiqueta de autenticación a su mensaje. Coste de autenticación en términos de material clave: 64.
- A informa a B sobre las bases que ella ha escogido para preparar los qubits y añade una etiqueta de autenticación a su mensaje. Coste de autenticación en términos de material clave: 64.

Fase 3.1: Reconciliación de la información - Valoración de Error Parcial:

A y B usan un esquema de valoración de error parcial. Ellos escogen 2 subconjuntos arbitrarios de prueba: el primero consistiendo en todas las medidas donde A y B han usado la base rectilínea y el segundo para aquellos donde usaron la base diagonal. Este esquema ofrece ventajas en lo que concierne a enfrentarse a un ataque específico como la estrategia de *escucha parcial disimulada*. Finalmente usan la tasa de error estimada para determinar si ellos deberían continuar con la transmisión y efectuar corrección de error cuántico, o si ellos deberían abortar el protocolo. Esto lo hacen basado en un umbral de tolerancia de error predefinido, por lo general alrededor del 11 %. Detalles:

- A y B permutan sus claves destiladas para reducir los errores a través de la cadena entera de bits. Realizan la valoración de error comparando un subconjunto de sus claves destiladas con error reducido.
- Una tasa de error de 0.1778 fue estimada usando una proporción de muestreo de 0.3.

Fase 3.2: Reconciliación de la información - Corrección de Error, algoritmo *Cascade*

A y B realizan un esquema de corrección de error interactivo conocido como el algoritmo Cascade sobre el canal público para localizar y corregir los bits erróneos en sus cadenas de bit destiladas. Detalles:

- La cascada ejecutada consiste en 7 rondas para corregir los errores.
- 25 bits erróneos fueron descubiertos y corregidos.
- 150 bits fueron perdidos para corregir los errores.
- Con una probabilidad de error de 0.1152, Shannon estipula que el número de bits perdidos es: 112.0, comparado al número real de bits perdidos: 150.

Fase 4: Confirmación de Corrección de Error y Autenticación

A y B confirman y autentican la fase de corrección de error mediante el cálculo del error en una porción de sus claves registradas, y comparando sus valores respectivos. Detalles:

- 64 bits de material clave fueron usados autenticar (la llave pre compartida secreta).
- El esquema universal hashing de Registro de desplazamiento de realimentación Lineal (LFSR) fue usado para la autenticación.

Fase 5: Amplificación de la privacidad

A y B calculan el escape total de la información y corren un protocolo de amplificación de privacidad para reducir al mínimo el conocimiento de E sobre la clave. Aplican un esquema universal hashing basado en matrices de Toeplitz. También pueden definir un parámetro de seguridad para reducir al mínimo el conocimiento de E a una cantidad arbitraria. Detalles:

- 182 bits fueron perdidos hasta este punto.
- La longitud clave antes de amplificación de la privacidad: 217 bits.
- La longitud final de la clave es: 15 bits.
- El parámetro de seguridad escogido es: 20.

Ver imagen 55 y referencia [26].

5.3. ANÁLISIS DE LA VERIFICACIÓN DEL PROTOCOLO E91

La tabla 6 registra el valor de los resultados de las figuras 59 a la 66, más el valor de la correlación <AB>:

Combinación de Medidas \ Código	P(0,0)	P(1,1)	P(0,1)	P(1,0)	*Correlación <AB>*
ZU	0,424	0,365	0,084	0,127	0,578
ZV	0,382	0,418	0,121	0,079	0,6
XU	0,472	0,335	0,102	0,09	0,615
XV	0,119	0,09	0,422	0,369	-0,582

Tabla 6. Resultados de correlación del estado de Bell.

El valor total de la correlación *C* entre los sistemas es:

$$|C| = |\langle ZU\rangle + \langle ZV\rangle + \langle XU\rangle - \langle XV\rangle| = |0{,}578 + 0{,}6 + 0{,}615 - (-0{,}582)| = \mathbf{2,375 \pm 0,004} \quad (65)$$

Los resultados son coherentes con los cálculos teóricos, así que de nuevo, queda demostrado, ahora por medios prácticos, la violación a la desigualdad de CHSH, es decir, la invalidez de los principios de *Realismo* y *Localidad* para estados entrelazados cuánticamente como el estado de Bell propuesto.

Esta violación, más los resultados del apartado anterior, permiten la creación de sistemas criptográficos basados en entrelazamiento cuántico, en un principio 100% seguros sin importar la distancia que separe a los dos sistemas correlacionados. Es un resultado importante considerando que las ejecuciones son efectuadas en procesadores cuánticos reales de IBM, y que demuestran propiedades únicas a la información cuántica entrelazada.

En la figura 69 se muestran los resultados de implementación como la anterior, ejecutados por ingenieros de los laboratorios de IBM.

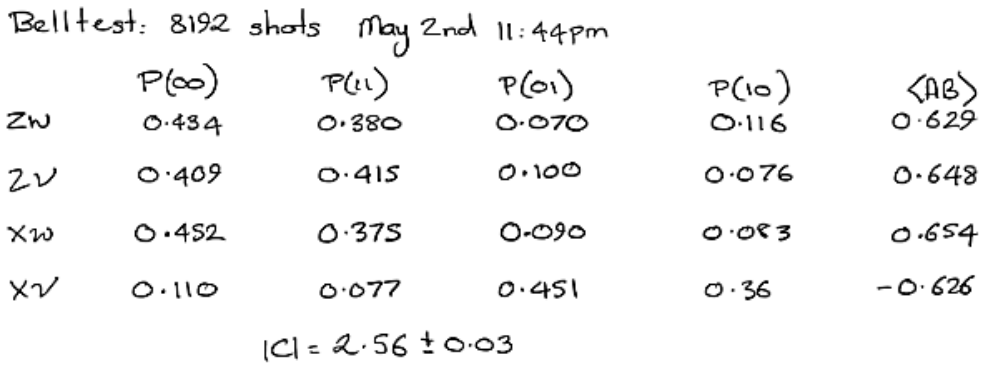


Figura 69. Prueba de Bell: 8192 ejecuciones. Mayo 2016 [29].

5.4. DIFERENCIA ENTRE LOS PROTOCOLOS

Como ya se vio, el QBER y el proceso de destilación de la clave en los dos protocolos es similar, ya que las fuentes de error y su influencia total son aproximadamente iguales. Sin embargo, difieren en otros aspectos relativos a la seguridad de la clave, como los establecidos al inicio de este trabajo: distribución, almacenamiento, codificación y ataques a la clave criptográfica por parte de terceros.

La criptografía cuántica, al igual que la criptografía asimétrica o de clave pública, nacen en respuesta al problema de distribuir la clave entre usuarios remotos de manera segura. Los protocolos BB84 y E91, al hacer uso de un canal cuántico, pueden monitorear en tiempo real el nivel de seguridad en la clave generada y estipular si la transmisión está siendo interceptada o no. Como su seguridad no se basa en complejidad computacional para desencriptar la clave, sino en fenómenos físicos, ambos protocolos se enfrentan con éxito al problema de distribuir la clave y codificarla.

Una diferencia importante entre los protocolos es que en el E91, el espía *E* no será capaz de detectar los estados de los qbits sin introducir errores en el correspondiente espacio del sistema, mientras que en BB84, E tiene la posibilidad, con cierta probabilidad, de medir los qbits sin cambiar sus estados, eligiendo la mismas bases de polarización en la que A preparo y envió los fotones. Teniendo en cuenta esto, se puede decir que la presencia de E es detectada con mayor facilidad en el protocolo E91.

Por otro lado, en el protocolo BB84, la clave creada por *A* y *B*, deberá ser almacenada por medios clásicos hasta que vaya ser usada junto con OTP. Así que sin importar que haya sido creada incondicionalmente segura frente a supervisión del canal, su seguridad continua a lo largo del tiempo solo será tan elevada como la seguridad de su almacenamiento. Mientras que usando el protocolo E91, los dos usuarios podrían preparar las partículas entrelazadas y luego medirlas para así crear la clave, justo en el momento en que la vayan a usar, eliminando por completo el problema del almacenamiento. Pero mantener un estado cuántico sin colapso es un problema complejo y muy estudiado hoy en día, denominado coherencia cuántica. La ventaja de este protocolo, es que la clave se genera "naturalmente al azar" ya que es imposible saber de antemano qué polarización tendrá cada fotón. Como se almacenan estados cuánticos en vez de clásicos, cualquier intento de medición de la clave, anterior a su uso, colapsará el sistema de estados entrelazados de Bell. Todo intento de espionaje a la clave almacenada podrá ser detectado inmediatamente por los usuarios. Por ello se estipula que la seguridad en el almacenamiento de la clave del protocolo E91 es superior, pero que debe enfrentarse a problema de coherencia.

En la práctica, realizar emisiones de un solo fotón no es algo sencillo de lograr. Generalmente los estados cuánticos son codificados en configuraciones diversas de fase o frecuencia, que no requieren el uso de fuentes de un solo fotón. Debido a ello las transmisiones de la criptografía cuántica usando el esquema BB84 podrían sufrir de ataques de tipo hombre en el medio. Adicionalmente cada componente del sistema de transmisión puede presentar errores que comprometan la seguridad de la clave.

El protocolo E91 debe usar una fuente generadora de fotones entrelazados. Debido a ello, está expuesto a una amenaza adicional con respecto al protocolo BB84. Es de vital importancia la fiabilidad que se tenga en la fuente generadora del par entrelazado (estados de Bell). Ésta, por lo general es controlada por alguno de los usuarios remotos *A* o *B*, pero en los casos en los que la fuente sea independiente, debe cuidarse de restringir su manipulación y supervisión, para que no caiga en manos de terceros. No obstante, *A* no necesita hacer elecciones aleatorias de bases de medición de los qbits, como en el paso 1 del protocolo BB84. Entonces un buen generador de números aleatorios no es necesario en el protocolo E91. Que *A* tenga que hacer al menos una elección aleatoria de las bases es una debilidad intrínseca del sistema.

En las implementaciones reales del protocolo BB84, puede haber fugas de información de la clave a canales secundarios o indirectos, como sonidos producidos por los componentes utilizados cuando hay

cambios en los qbits o en las bases usadas, entre otros canales. Con el protocolo E91, si dos partes están entrelazadas entonces no puede haber fuga de información por medio de ningún canal secundario.

A pesar de que es difícil establecer cuál de los protocolos es más seguro sin analizar una situación específica, la naturaleza de la clave y de la implementación práctica del protocolo E91, hacen que el sistema completo este menos expuesto a ataques o fugas de información sobre la clave.

5.5. REALIDAD

De la misma manera que la tecnología del diseño de microprocesadores ha evolucionado hasta llegar o meter millones de transistores en diminutas tarjetas milimétricas, y que la información en sea configurada por 1s y 0s que son la existencia o no de un sencillo electrón en las compuertas de un transistor, también hoy en día se pueden transmitir fotones simples uno por uno a través de un cable de fibra óptica. Ambos avances han permitido el desarrollo de la computación y la criptografía cuántica. IBM utiliza qbits de superconducción sobre tarjetas de silicona de la misma tecnología usada en microprocesadores hoy en día, para hacer computación cuántica. Toshiba utiliza la polarización del fotón y las leyes de la física para crear sistemas de comunicación basados en criptografía cuántica. Quien sabe en un futuro que otros tipo de tecnologías se desarrollen basados en física y computación cuántica.

David Deutsch fue el pionero de la computación cuántica y el primero en proponer el entrelazamiento cuántico como base para la distribución de clave cuántica. Esta idea fue posteriormente desarrollada por Arthur Eckerd, quien publico la posibilidad de la criptografía cuántica violando la desigualdad de Bell.

El interés ha venido creciendo en la última década, y por ende la tecnología ha evolucionado desde el primer aparato "hecho en casa" por Bennet y Brassard y Eckerd como coautor para probar que su teoría de comunicación funcionaba (Figura 1); y hoy en día existen varias implementaciones de sistemas de criptografía cuántica, que como ya se había dicho, aplican la distribución de llave cuántica más alguna técnica de uso de la llave como el cuaderno de un solo uso y/o certificados que verifiquen la identidad de los usuarios. Estos sistemas funcionan actualmente en redes con estándares de seguridad altos y como sustento de pruebas para mejorar la eficiencia de este tipo de transmisión encriptada, que bajo la protección de los principios de la física cuántica será una tecnología muy importante en el futuro.

El primer prototipo de QKD, creado en 1989, funcionaba a una distancia de 32 centímetros. Uno de los sistemas demostrados más veloces, alcanzado por Toshiba y la Universidad de Cambridge, usando el protocolo BB84 con *estados de señuelo*[31], comparte claves cuánticas entre usuarios a una tasa de 1Mbit/s, a través de 20 Km de fibra óptica, y de 10Kbit/s a 100 Km. En Marzo del 2007 se demostró la funcionalidad de QKD a una distancia record de 148.7 Km por fibra óptica, gracias a los esfuerzos del Laboratorio Nacional Los Álamos y NIST[32], usando igualmente el protocolo BB84. La distancia record para intercambio de clave por espacio libre es de 144 Km, entre dos de las Islas Canarias, lograda en 2006 por una colaboración Europea, usando fotones entrelazados (esquema E91), y usando estados de señuelo (BB84) en el 2007. Los experimentos sugieren que la transmisión a satélites de esta manera también es posible.

Hoy en día existen varias implementaciones funcionales de ser redes o sistemas mixtos de criptografía cuántica y simétrica o asimétrica, y otras de prueba para explorar la aplicabilidad de los sistemas de distribución de clave cuántica. Típicamente hay dos perfiles de aplicación de la criptografía cuántica: la primera es un sistema que crea un flujo de datos encriptado bajo un modelo cliente/servidor y la segunda

[31] Buscar
[32] Instituto Nacional de Estándares Y Tecnología

es la creación de una red privada virtual (VPN - *Virtual Private Network*) punto a punto sobre IPSec (*Internet Protocol Security*). La figura 70 muestra una red de acceso cuántica creada por Toshiba [36].

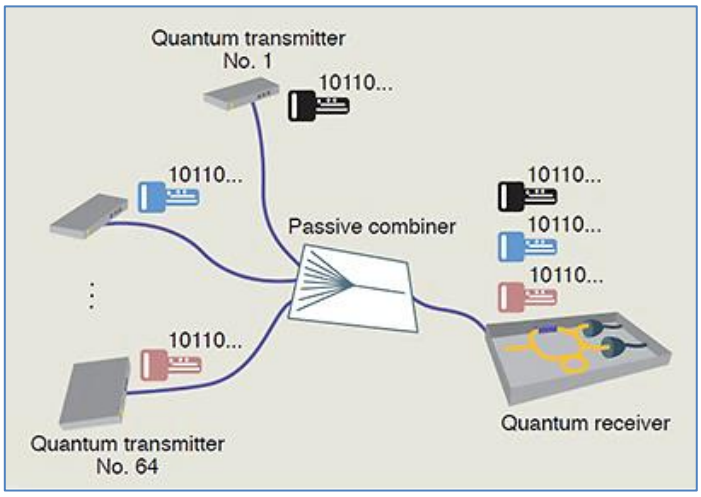


Figura 70. Red de acceso cuántica de Toshiba.

En Toshiba, usan tecnología de red óptica pasiva (PON), para conectar múltiples usuarios en una arquitectura de árbol, permitiendo compartir un detector de fotón sencillo, (el cual es uno de los componentes más complejos y costosos dentro del sistema de transmisión y cuántica) entre los usuarios receptores. Han demostrado que su detector puede ser compartido hasta con 64 usuarios. Técnicas de estabilización activa proveen una operación continua y estable de la red. Se pueden transferir aproximadamente 256 qbits de encripción secreta por segundo, en una red de 8 usuarios. Este alcance logrado muestra el camino de las primeras tecnologías que implementan la criptografía cuántica en aplicaciones de redes inteligentes.

En la práctica, realizar emisiones de un solo fotón a la vez es algo muy difícil, y en últimas muy costoso. Adicionalmente el canal cuántico debe lidiar con problemas de coherencia Es por esto que los estados de la base, son codificados generalmente mediante configuraciones para $|0>$ *y* $|1>$, diferentes a una estipulada solo por la polarización del fotón como se detalla en el titulo con el mismo nombre (marco teórico). Tres de las más usadas son conocidas como[33]:

- Estado señuelo del fotón.
- Estado señal del fotón.
- Estado en sobre de pulsos.

En el estado señuelo, los qbits son transmitidos usando niveles de intensidad diferentes en las fuentes de transmisión. En el estado señal del fotón, se logra una distribución gaussiana con múltiples fotones. En el estado de sobre de pulso, un porcentaje del fotón (encerrado en un sobre), pasa por una línea de atraso óptica, es decir, se logra una desviación de una parte del fotón por una línea de fibra óptica de longitud *L* para generar un atraso y así tener un pulso doble fotónico en un sobre de longitud *l*.

Un ejemplo de una aplicación usando el estado sobre de pulsos es una red que existe en Japón, creada por Toshiba y los el NICT ().

En su sistema de distribución de clave cuántica, el fotón es preparado en un sobre de pulso, que mide aproximadamente 1cm, confinado en fibra óptica. La figura 71 muestra el sobre de pulso original:

[33] *Decoy state, signal state* y *pulse envelop.*

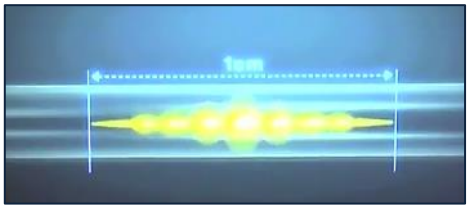


Figura 71. Sobre de pulso de 1cm (Toshiba).

Este fotón pasa por un circuito óptico con un ciclo de retraso que divide al fotón en dos, separado por 10cm debido a que produce un atraso (Figura 72).

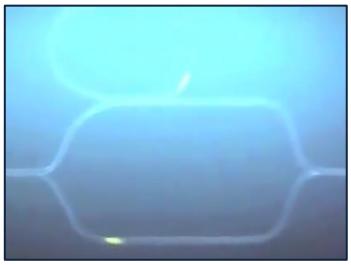


Figura 72. Circuito óptico generador de atraso.

El estado del pulso final es una configuración de sobre de doble pulso, como se ve en la figura 73. Un sencillo fotón existe entonces en este sobre de pulso doble:


Figura 73. Sobre de pulso doble.

El sobre de pulsos es luego modulado para obtener los estados de la base $\{|0>,|1>\}$. La figura 74, muestra la base modulada en la configuración de pulso doble descrita:

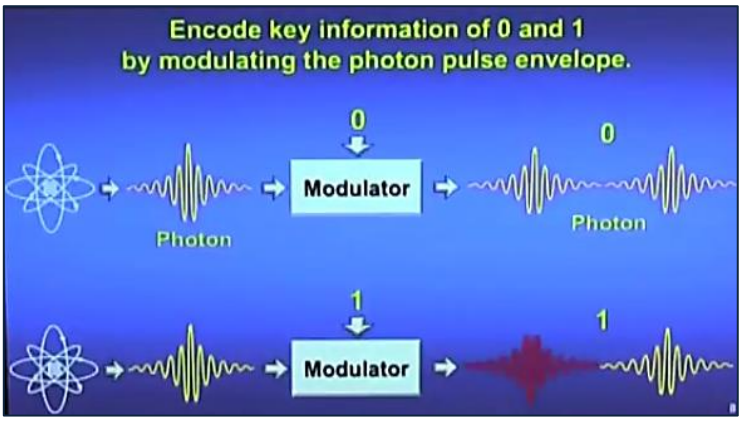


Figura 74. Sobre de pulso doble modulado en 0 y 1 lógicos.

Es importante recordar que un fotón es la partícula fundamental de la luz, por la tanto este no se puede dividir en más partes. Las dos fases corresponden a energías equivalentes a fracciones de un fotón.

Luego el fotón entra en un modulador óptico, que modifica su sobre de pulso acorde con la información que se quiere transmitir, creando la primera base de codificación (Figura 75):

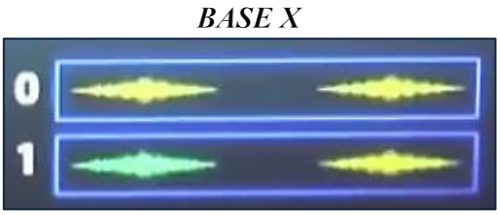


Figura 75. Modulación de sobre de pulso doble en base X. Toshiba.

El cero se representa por el par de pulsos que está en fase y el uno por el par que no lo está. Esto permite la transmisión de fotones a una larga distancia, porque dos pulsos en la fibra óptica experimentan las mismas perturbaciones, las cuales pueden ser canceladas en el sistema del receptor.

Ahora, para detectar espionaje, preparan otro sobre de pulsos. En el segundo sobre la información de codifica de la siguiente manera, creando la segunda base de codificación de la información (Figura 76):

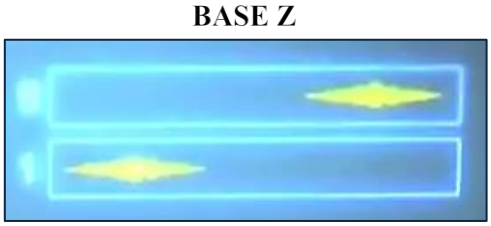


Figura 76. Modulación de sobre de pulso doble en base X. Toshiba.

Estas dos bases representan las dos propiedades que no pueden ser determinadas al mismo tiempo según el principio de incertidumbre de Heisenberg. Medir un fotón en una base incorrecta hará que esta cambie, y por ende que la información codificada presente errores inmediatos.

Los unos y ceros son generados aleatoriamente y codificados en las bases de sobres de pulsos de fotón mencionadas anteriormente. Estos pulsos superpuestos no pueden ser copiados sin errores, esto es conocido como el principio de no clonación.

Para detectar el espionaje al final comparten cierta cantidad de bits trasmitida y recibida. Se aplican técnicas de destilación de la clave, amplificación privada y corrección de error. Después de generada la clave, es usada una vez y desechada como cuaderno de un solo uso. Hoy en día generan claves y transmiten texto cifrado a distancias de 45 Km de fibra óptica.

6. CONCLUSIONES

Es cuestión de tiempo que los primeros computadores cuánticos, que permitan ejecutar algoritmos como el de Shor, para factorizar números primero en un tiempo polinomial, representen una amenaza para los esquemas criptográficos más usados hoy en día por todos. Como solución a este y otros problemas, se justifica aplicación de la criptografía cuántica, y es por eso que ya existen empresas dedicadas a crear redes seguras usando el *cuaderno de un solo uso* y la criptografía cuántica. Sin embargo existen otros esquemas de criptografía *post-cuántica*[34] , que se refieren a investigaciones en sistemas criptográficos, usualmente de criptografía asimétrica, que no sean quebrantables por computadores cuánticos usando algoritmos que aprovechan principios de la física cuántica como el algoritmo de Shor. Son obvias las razones por las que ésta se ha vuelto una área de mucho interés investigativo, para la grupos que requieran estándares de seguridad muy altos (como entidades gubernamentales y militares), y por ende para mayoría de empresas dedicadas a la seguridad de la información.

La superposición de estados cuánticos, es uno de los aspectos más importantes de esta tecnología. Es debido a esto que en la implementación de los algoritmos, es posible que dos ramas de una sentencia condicional pueden ser ejecutadas al mismo tiempo. Este y otros fenómenos físico-cuánticos nombrados a lo largo del trabajo, cambian totalmente la manera concebir el computo programable dentro un procesador. Las herramientas digitales de simulación son una experiencia útil para ejecutar protocolos de prueba, de posibles implementaciones futuras.

QKD es una nueva y poderosa herramienta dentro de la transmisión de información de manera segura entre usuarios remotos, que muy seguramente se volverá imponente en los próximos años, ya que le permite acordar una clave segura que será utilizada en la transmisión de un mensaje privado, por medio de un canal inseguro, siendo independiente de cualquier valor de entrada; algo imposible para la criptografía convencional (clásica). La mayor diferencia frente a la criptografía solo por medios clásicos, es que en la cuántica, toda supervisión del canal es activa, otorgándole la habilidad al sistema de detectar automáticamente cualquier intercepción en la transmisión, aumentando la fiabilidad y reduciendo costos al no tener que recurrir a *mensajeros* y a técnicas para asegurar la seguridad de la transmisión. Estos sistemas no dejan de estar expuestos a criptoanalistas cuánticos y a ataques de otro tipo a los que atañen a la criptografía convencional. Sin embargo, esto solo hará que las técnicas y los dispositivos utilizados para realizar y proteger la información, sean cada vez más especializados y eficientes.

Avances logrados como el detector fotónico y la red de Toshiba [36]; redes cuánticas de acceso, e implementaciones de QKD en redes inalámbricas [37]; son esenciales para hacer la criptografía cuántica, más práctica, accesible y menos costosa. Es de esperarse que en los próximos años se logren sistemas más veloces y robustos, que permitan una implementación más general de la criptografía cuántica, para proteger información sensible de los usuarios, como por ejemplo, datos médicos e información del genoma humano de una persona.

La principal diferencia entre los tipos de criptografía cuántica en los que se basan los protocolos BB84 y E91, es que en el primero *A* y *B* deberán guardar la clave generada (teóricamente 100% segura) en sus computadores. El problema es que *E* podría quebrantar la seguridad de sus sistemas y mirar en la clave almacenada sin detección alguna. Así que la seguridad de la clave estará supeditada a la seguridad en su almacenamiento (que es por medios clásicos y criptografía convencional). En teoría, en el protocolo E91, los estados entrelazados de los fotones, pueden ser almacenados por un tiempo indefinido sin nunca ser observados. Si *E* llegara a verlos, *A* y *B* lo sabrían automáticamente. En la práctica, este protocolo se debe enfrentar a problemas de coherencia en los estados cuánticos. La tecnología actual aun no permite

[34] Sistemas criptográficos cuya seguridad no puede ser violada por computadores cuánticos.

almacenamiento de cadenas de qbits en estados superpuestos por tiempos indefinidos. Debido esto, las implementaciones del protocolo BB84 son más populares y han demostrado mayor progreso.

Aunque la criptografía cuántica no sea muy práctica hoy en día, es la rama de la computación cuántica que más presenta avances y que tiene implicaciones más severas en sus resultados. A diferencia de los sistemas criptográficos asimétricos, su seguridad ha sido demostrada 100% segura sin importan con qué recursos computacionales se cuente. Actualmente funciona entre distancias cortas (útil dependiendo de la aplicación). Con un poco más de avance técnico, se logrará la implementación de redes de comunicación que transmitan mensajes secretos entre usuarios separados por distancias más largas. Las diferencias conceptuales y funcionales que presenta con otras técnicas criptográficas, alientan a la investigación y exploración de ideas nuevas para proteger la información.

7. BIBLIOGRAFÍA

[1] Norma técnica colombiana NTC-ISO/IEC 27001, "Tecnología de la información. Sistemas de gestión de la seguridad de la información SGSI. Requisitos", 2006. Disponible en línea: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[2] Re-Orientation, Fundamentos sobre criptografía, L. Nieto, 2010. Disponible en línea: http://www.re-orientation.com/fundamentos-criptografia

[3] Cifrado asimétrico-Algoritmo RSA, memorias de un aprendiz de php. Disponible en línea: http://www.rinconastur.com/php/php20.php

[4] Khan Academy labs, Time Complexity, 2008. Disponible en línea: https://www.khanacademy.org/labs/explorations/time-complexity

[5] Urrego Nelson. Pontificia Universidad Javeriana, 2006. "Seguridad criptográfica y criptografía cuántica".

[6] IBM Quantum Computing, Quantum Experience, user guide, 2016. Disponible en línea: https://quantumexperience.ng.bluemix.net/qstage/#/tutorial?

[7] Khan Academy, el algoritmo de Euclides, 2016. Disponible en línea: https://es.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/the-euclidean-algorithm

[8] Wikipedia, experimento de Young, 2016. Disponible en línea: https://es.wikipedia.org/wiki/Experimento_de_Young

[9] Wikipedia, notación bra-ket, 2016. Disponible en línea: https://es.wikipedia.org/wiki/Notaci%C3%B3n_bra-ket

[10] Francisco R. Villatoro, "Medida de la trayectoria en la esfera de Bloch de un cubit superconductor", 2015. Disponible en línea: http://francis.naukas.com/2014/07/31/medida-de-la-trayectoria-en-la-esfera-de-bloch-de-un-cubit-superconductor/

[11] Ruíz Jiménez, Carlos, computación cuántica, algoritmo de Simon, 2016. Disponible en línea: http://www.fisicafundamental.net/misterios/computacion.html#simon

[12] Paul Baecher. Darmstadt University of Technology, 2014. "Simon's Circuit, a note on Cleverly-Chose Circuits". Disponible en línea: https://eprint.iacr.org/2014/476.pdf

[13] M Olmo, R Nave. Clasificación de la polarización, 2000. Disponible en línea: /http://hyperphysics.phy-astr.gsu.edu/hbasees/phyopt/polclas.html#c1.

[14] Criptografía cuántica – principio y algoritmos. Disponible en línea: http://www.textoscientificos.com/criptografia/criptoquantica

[15] Einstein, A, Podolsky, B, & Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" Physical Review, (1935). 47(10), 777-780.

[16] Lo, H. -K, & Zhao, Y. Quantum Cryptography,". Disponible en línea: http://arxiv.org/abs/0803.2507/

[17] Wikipedia, coherencia cuántica, 2015. Disponible en línea: https://es.wikipedia.org/wiki/Coherencia_cu%C3%A1ntica

[18] Pradilla Cerón, Juan Vicente. Grupo de comunicaciones ópticas y cuánticas del iTEAM. "Destilación de clave cuántica", 2012. Disponible en línea: https://riunet.upv.es/bitstream/handle/10251/33251/Memoria_Pradilla_Juan.pdf?sequence=1

[19] Wikipedia, entropía (información), 2016. Disponible en línea: https://es.wikipedia.org/wiki/Entrop%C3%ADa_(informaci%C3%B3n)

[20] Xiaoqing Tan, Dept. of Mathematics, Jinan University, Guangzhou, Guangdong, China. "Introduction to Quantum Cryptography", 2013. Disponible en línea: http://cdn.intechopen.com/pdfs-wm/43793.pdf

[21] Criptografía cuántica, 2013. Disponible en línea: http://www.esi2.us.es/DFA/IIC/archivos/FIC1213/5-Criptografia%20Cuantica-12-13.pdf

[22] Wikipedia, función hash criptográfica, 2016. Disponible en línea:
https://es.wikipedia.org/wiki/Funci%C3%B3n_hash_criptogr%C3%A1fica
[23] "IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation", IBM press release, 2016. Disponible en línea: http://www-03.ibm.com/press/us/en/pressrelease/49661.wss
[24] IBM Quantum Computing, Quantum Experience, user guide, The Quantum Composer, 2016. Disponible en línea:
https://quantumexperience.ng.bluemix.net/qstage/#/tutorial?sectionId=75a85f7e14ae3fd4329ad5c3e59466ea&pageIndex=3
[25]Google, Quantum Computing Playground, 2014. Disponible en línea:
http://www.quantumplayground.net/#/about
[26] Arash Atashpendar, QKD Simulator, "Simulation and Analysis of QKD (BB84)", 2014. Disponible en línea: https://www.qkdsimulator.com/simulate
[27] Igor L. Markov, Mehdi Saeedi. Cornell University Library. "Constant-Optimized Quantum Circuits for Modular Multiplication and Exponentiation", 2012. Disponible en línea:
https://arxiv.org/abs/1202.6614
[28] La polarización de la luz, la óptica. Disponible en línea:
http://opticamarioralejandroc11a.blogspot.com.co/2011/10/la-polarizacion-de-la-luz.html
Imagen http://www.grincef.nurr.ula.ve/EULA-2007/Polarizaci%F3n/contenido/polarizacion_12a.htm
[29] IBM Quantum Computing, Quantum Experience, user guide, Shor's algorithm, 2016. Disponible en línea:https://quantumexperience.ng.bluemix.net/qstage/#/tutorial?sectionId=8443c4f713521c10b1a56a533958286b&pageIndex=6
[30] Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". Disponible en línea:
http://arxiv.org/abs/quant-ph/9508027.
[31] Wikipedia, teoría de la complejidad computacional, 2016. Disponible en línea:
https://es.wikipedia.org/wiki/Teor%C3%ADa_de_la_complejidad_computacional#Algoritmos_de_tiempo_polin.C3.B3mico_y_problemas_intratables
[32] John Proos, Christof Zalka. Cornell University Library. "Shor's discrete logarithm quantum algorithm for elliptic curves", 2003. Disponible en línea: https://arxiv.org/abs/quant-ph/0301141
[33] Andrés Sicard R., Mario Elkin Vélez R. Departamento de ciencias básicas, universidad EAFIT, Medellín, Colombia, 1999. Disponible en línea: http://www1.eafit.edu.co/asr/pubs/icq.pdf
[34] Cormick, Cecilia. Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires. "Funciones de Wigner discretas y estados estabilizadores en computación cuántica", 2005. Disponible en línea: http://qufiba.df.uba.ar/theses/ThesisCormick.pdf
[35] "Elementary gates for quantum computation", Physical review A, American Physical Society, 1995. Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Disponible en línea:
http://journals.aps.org/pra/abstract/10.1103/PhysRevA.52.3457?cm_mc_uid=43781767191014577577895&cm_mc_sid_50200000=1460741020
[36] Toshiba, decoy state network, 2015. Disponible en línea:
http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system/
[37] Xu Huang, Shirantha Wijesekera, Dharmendra Sharma. Universidad de Camberra, Australia, 2008. "Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802.11) Wireless Networks". Disponible en línea: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.1543&rep=rep1&type=pdf
[38] R. Rivest, A. Shamir, L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Publicación inicial del esquema RSA. Disponible en línea: http://people.csail.mit.edu/rivest/Rsapaper.pdf
[39] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, y Clifford Stein. "Introduction to Algorithms", tercera edición. Sección 31.7: The RSA public-key cryptosystem, pp.960-989. Disponible en línea:http://ce.bonabu.ac.ir/uploads/30/CMS/user/file/115/EBook/Introduction.to.Algorithms.3rd.Edition.Sep.2010.pdf

ANEXOS

A. CIRCUITOS CUÁNTICOS

La unidad fundamental de información cuántica es el bit cuántico o *qbit.* Es generado por los elementos de la base ortonormales, cuya representación matricial (2 x 1), como se ve en [33] es:

$$|0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

La forma generalizada del vector de onda que describe el estado del qbit es:

$$|\psi> = a_0\,|0> + a_1\,|1>$$

donde $a_0, b_0 \in \mathbb{C}$ y:

$$|a_0|^2 + |a_1|^2 = 1$$

Un espacio conformado por dos qbits esta descrito por:

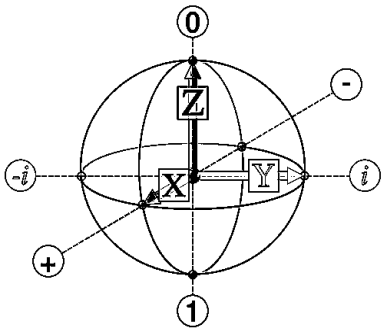
$$|\psi_1> \otimes |\psi_2> = |\psi_1, \psi_2> = a_0\,|0,0> + a_1\,|0,1> + a_2\,|1,0> + a_3\,|1,1>$$

Las bases de medición esenciales que atañen a este informe son:

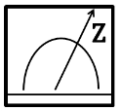
$$\textit{Rectilinea}\ |0> y\ |1> \quad \textit{Base}\ 1 \longleftrightarrow \begin{cases} |\psi_0\rangle = |0\rangle \\ |\psi_1\rangle = |1\rangle \end{cases}$$

$$\textit{Diagonal}\ |+> y\ |-> \quad \textit{Base}\ 2 \longleftrightarrow \begin{cases} |\psi_+\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \\ |\psi_-\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right] \end{cases}$$

Las bases descritas pueden ser ilustradas mediante la esfera de Bloch:



Una medición sobre la base 1, se interpreta como una medición sobre el eje Z de la esfera de Bloch
.



Si se realiza una medida sobre el sistema $|\psi> = a_0\,|0> + a_1\,|1>$ sobre la base $|\psi_+> = \left\{\frac{1}{\sqrt{2}}(|0> + |1>)\right\}$, se genera la probabilidad:

$$P\left(\frac{1}{\sqrt{2}}(|0> + |1>)\right) = \left|\frac{1}{\sqrt{2}}(a_0 + a_1)\right|^2$$

De modo que si $a_0 = 1$ y $a_1 = 0$:

$$|\psi> = 1\,|0>$$

y la probabilidad de medición del qubit sobre la base descrita será:

$$P\left(\frac{1}{\sqrt{2}}(|0> + |1>)\right) = \left|\frac{1}{\sqrt{2}}1 + 0\right|^2 = 0{,}5 = \mathbf{50}\%$$

Lo anterior descrito es equivalente a hacer una medición sobre la base diagonal (Figura 14) a un fotón que se encuentra polarizado en 0º (base rectilínea).

La evolución o dinámica del estado de un qbit está determinada por un operador unitario sobre el espacio del sistema cuántico, llamado espacio de Hilbert. Una matriz es unitaria si su matriz adjunta es igual a su inversa, lo cual es equivalente a decir que:

$$U^t * U = \mathbb{I}$$

donde U^t es la transpuesta conjugada de la matriz compleja U , y $\mathbb{I}$ es la matriz identidad.

Aplicar una compuerta cuántica equivale a una transformación unitaria sobre el espacio del sistema, dándoles la particularidad de ser reversibles. Un circuito cuántico, es un conjunto de operadores unitarios, aplicados a uno o más qbits, para cambiar su estado inicial a un estado *primado:*

$$U * |\psi> = |\psi'>$$

El resultado de un circuito cuántico siempre estará determinado por algún tipo de medición sobre el sistema, que provocara el colapso de la función de onda.

Las compuertas cuánticas para un solo qbit, tienen asociadas matrices 2 x 2. Pueden ser interpretadas como rotaciones sobre los ejes de la esfera de Bloch: X, Y, y Z. Un ejemplo de ellas son los operadores de Pauli:

$$U_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$U_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$U_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

El eje Z corresponde a la base $\{|0>, |1>\}$, por lo que aplicar el operador Z a un qbit que este en la base, no significa ningún cambio en el estado cuántico; pero aplicar una compuerta X, equivale a una rotación de π radianes sobre el eje X de la esfera de Bloch, lo que culmina en cambiar el estado $|0>$ por el estado $|1>$, y viceversa. Es por ello que la compuerta X es también conocida como la compuerta NOT cuántica, siempre el qbit se encuentre en la base 1.

SUPERPOSICIÓN

Una de las compuertas más importantes en computación cuántica es la compuesta Hadamard. Esta compuerta transforma a un qbit en una superposición de dos elementos de la base $\{|0>, |1>\}$. La matriz que la representa es:

$$U_{HADAMARD} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Así que la transformación sobre los elementos de la base queda descrita por:

$$U_{HADAMARD}|0> = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0> + |1>)$$

$$U_{HADAMARD}|1> = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0> - |1>)$$

De modo que para pasar un qbit que se encuentra en la base $\{|0>, |1>\}$ (polarización rectilínea 0º, 90º), a la base $\left\{ \frac{1}{\sqrt{2}}(|0> + |1>), \frac{1}{\sqrt{2}}(|0> - |1>) \right\}$ (polarización diagonal 45º, 135º), se debe aplicar el operador Hadamard. De la misma manera, para realizar mediciones en una base diagonal, se debe transformar la medición en Z sobre la esfera de Bloch, a una medición en X.

Muchos algoritmos cuánticos usan la compuerta Hadamard al comienzo, para pasar *n* qbits que se encuentran en el estado $|0>^{\otimes n}$, a una superposición de 2^n estados ortogonales con igual peso ($\frac{1}{2^n}$).

Otra manera de lograr superposición es mediante compuertas de desplazamiento de fase. Su forma matricial es:

$$U_{R(\theta)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Estos operadores dejan el estado base $|0>$ intacto y asignan el $|1>$ a $e^{i\theta}|1>$. La probabilidad de medir un $|0>$ o un $|1>$ no cambia después de aplicar esta compuerta, sin embargo, sí modifican la fase del

estado cuántico. Esto es equivalente a trazar un círculo horizontal (una línea de latitud) sobre la esfera de Bloch de θ radianes. Se muestran resultados para diferentes θ de desplazamiento:

$$\theta = \pi \rightarrow \ U_{R(\pi)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = U_Z$$

$$\theta = \frac{\pi}{2} \rightarrow \ U_{R(\frac{\pi}{2})} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = U_S$$

$$\theta = \frac{3 * \pi}{2} \rightarrow \ U_{R(\frac{3*\pi}{2})} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i*3\pi}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = U_{S^t}$$

Una medición equivalente al eje Y en la esfera de Bloch esta descrita por:

Las compuertas descritas anteriormente (X, Y, Z, H, S, S^t) son conocidas como como compuertas de Clifford, son transformaciones unitarios sobre un solo 1bit y pueden ser simuladas eficientemente en un computador clásico, como lo describe el teorema de Gottesman-Knill [34]. De manera general, una compuerta cuántica que opera sobre un único qbit puede ser representada por:

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$$

Las compuertas que no hacen parte de este grupo son únicas en este tipo de computación, y son muy usadas por la mayoría de los algoritmos cuánticos que resuelven problemas muy difíciles o imposibles para un computador clásico.

Los estados conformados por un sistema de 2 qbits son matrices de dimensiones 4 x 1:

$$|0,0> = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |0,1> = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|1,0> = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |1,1> = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Las matrices de operadores sobre dos qbits son de dimensión 4 x 4. Ejemplo de compuertas de 2 qbits son la XOR o CNOT cuántica (*C* de control o condición) y la compuerta SWAP, en las cuales, las trasformaciones de un qbit están determinadas por el comportamiento del otro. Las compuertas de dos qbits no podrán ser representadas de la misma manera por la esfera de Bloch, ya que las dimensiones del sistema compuesto por 2 qbits, exceden las dimensiones XYZ de la esfera. Solo son posibles resultados en barras probabilísticas (para el *IBM Quantum Experience*).

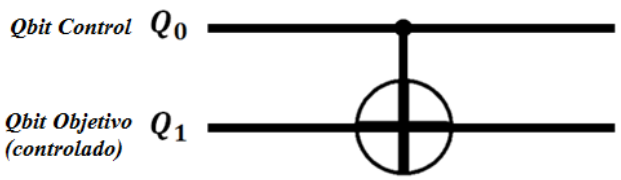
La compuerta XOR o CNOT, permite hacer lógica condicional. Ejecuta el operador *Ux dependiendo del valor del qbit de control.*

$$U_{XOR} = U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

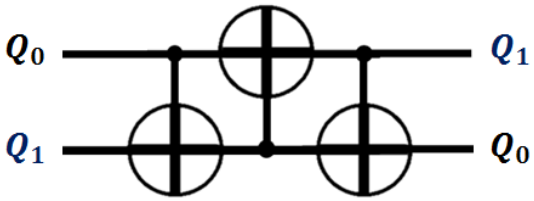
La compuerta SWAP aplica una transformación unitaria sobre el sistema de dos qbits, logrando que ambos cambien sus posiciones, es decir:

$$U_{SWAP}(Q_3 Q_4) = Q_4 Q_3$$

$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



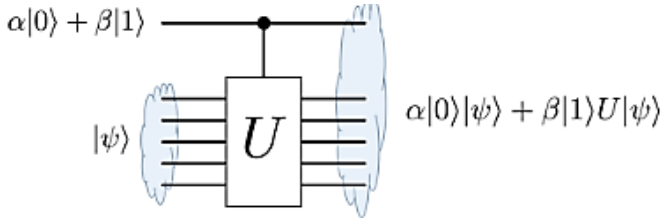
La transformación SWAP no hace parce del paquete básico de compuertas cuánticas que utilizan la mayoría de los procesadores (reales o simulados). Ésta, puede ser construida a partir de 3 compuertas CNOT como sigue:



La forma matricial general de una transformación unitaria sobre un qbit, controlada por otro es:

$$C(U) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

El primer qbit actúa como el controlador. El objetivo de control puede ser otro qbit o un registro de ellos. El control se puede aplicar incluso a una transformación unitaria U como se muestra en la figura:



Las compuertas lógicas AND y NOT son llamadas compuertas lógicas universales, porque cualquier función f: {0, 1} n → {0, 1} m puede ser implementada en un circuito lógico que utilice solo estas compuertas. Por otro lado, no es posible obtener un conjunto de compuertas universales para funciones reversibles de la forma f: {0, 1} n → {0, 1} n con compuertas reversibles de 1-bit ni con compuertas reversibles de 2-bits; un conjunto de compuertas universales reversibles está formado por un compuertas de 3-bits como la compuerta de Toffoli, también conocida como CCNOT, Y la compuerta Fredkin, también conocida como CSWAP.

Sin embargo, en computación cuántica, toda matriz unitaria puede ser escrita como una combinación de compuertas de uno y dos qbits, si agregamos al menos alguna no perteneciente al conjunto de compuertas tipo Clifford [35]

Una de las opciones más populares para compuertas cuánticas que no hagan parte del grupo Clifford es una compuerta que aplique un desplazamiento de fase $U_{R(\theta)}$ con $\theta = \frac{\pi}{4}$ o con $\theta = \frac{7\pi}{4}$:

$$\theta = \frac{\pi}{4} \rightarrow \ U_{R(\frac{\pi}{4})} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1+i) \end{pmatrix} = U_T$$

$$\theta = \frac{7 * \pi}{4} \rightarrow U_{R(\frac{7*\pi}{4})} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i*7\pi}{4}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1-i) \end{pmatrix} = U_{T^t}$$

Con esta compuerta adicional se hace posible alcanzar cualquier punto sobre la esfera de Bloch.

B. CÓDIGO DEL ALGORITMO DE SHOR

El código es provisto públicamente por Google y se encuentra en el *QuantumPlayground* [25]. Está escrito en lenguaje Qscript basado en C++:

```
// Based on C++ code from libquantum library.

proc FindFactors N
x = 0

 if N < 15
  Print "Invalid number!"
  Breakpoint
 endif

 width = QMath.getWidth(N)
 twidth = 2 * width + 3

 for x; (QMath.gcd(N, x) > 1) || (x < 2); x
  x = Math.floor(Math.random() * 10000) % N
 endfor

 Print "Random seed: " + x

 for i = 0; i < twidth; i++
  Hadamard i
 endfor

 ExpModN x, N, twidth  // Aquí se ejecuta la función exponenciación modular

 for i = 0; i < width; i++
  MeasureBit twidth + i
 endfor

 InvQFT 0, twidth  // Aquí se ejecuta la transformada inversa cuántica de Fourier

 for i = 0; i < twidth / 2; i++
  Swap i, twidth - i - 1
 endfor

 for trycnt = 100; trycnt >= 0; trycnt--
  Measure
  c = measured_value

  if c == 0
   Print "Measured zero, try again."
   continue
  endif

  q = 1 << width

  Print "Measured " + c + " (" + c / q + ")"

  tmp = QMath.fracApprox(c, q, width)
```

```
    c = tmp[0];
    q = tmp[1];

    Print "fractional approximation is " + c + "/" + q

    if (q % 2 == 1) && (2 * q < (1 << width))
      Print "Odd denominator, trying to expand by 2."
      q *= 2
    endif

    if q % 2 == 1
      Print "Odd period, try again."
      continue
    endif

    Print "Possible period is " + q

    a = QMath.ipow(x, q / 2) + 1 % N
    b = QMath.ipow(x, q / 2) - 1 % N

    a = QMath.gcd(N, a)
    b = QMath.gcd(N, b)

    if a > b
      factor = a
    else
      factor = b
    endif

    if (factor < N) && (factor > 1)
      Display "<h2>Success: " + factor + " " + N / factor
      Breakpoint
    else
      Print "Unable to determine factors, try again."
      continue
    endif
  endfor
endproc

VectorSize 22
FindFactors 437
```