Desarrollo de un simulador para el protocolo de criptografía cuántica E91 en un ambiente distribuido

Development of a simulator for the quantum cryptography protocol E91 in a distributed environment

Luis Cáceres Alvarez[1] Roberto Fritis Palacios[1] Patricio Collao Caiconte[1]

Recibido 18 de junio de 2014, aceptado 6 de octubre de 2014
Received: June 18, 2014 Accepted: October 6, 2014

RESUMEN

El objetivo del presente trabajo de investigación, consiste en el desarrollo de una aplicación que sea capaz de simular el comportamiento de uno de los principales protocolos de criptografía cuántica desarrollados, el protocolo E91. Para lograr dicho objetivo fue fundamental una investigación exhaustiva de los principales conceptos, principios y teoremas de la mecánica cuántica, como además del estudio de otros protocolos de criptografía cuántica y su desarrollo en la actualidad. Con toda la información recopilada se procede al desarrollo de la aplicación, empezando por la definición de los requerimientos, luego se continúa con la implementación y las posteriores pruebas de la aplicación, que permite compilar todo el trabajo de análisis y diseño realizado. Los resultados obtenidos, demostraron las fortalezas y debilidades de la aplicación para la distribución segura de una clave final cuántica. Si bien este trabajo es principalmente de investigación, el desarrollo de la aplicación que simula el comportamiento del protocolo E91, es de carácter esencialmente demostrativo.

Palabras clave: Mecánica cuántica, criptografía cuántica, protocolo cuántico E91, simulador E91, programación distribuida, RMI.

ABSTRACT

The objective of this research work is the development of an application which is capable of simulating the behavior of one of the main developed protocols of quantum cryptography, the protocol E91. In order to achieve this objective, it was essential to carry out an exhaustive investigation of the main concepts, principles and theorems of quantum mechanics; as well as the study of other quantum cryptographic protocols and their development today. With all the collected information, the development of the application begun, starting with the definition of the requirements, then implementing and subsequently testing the application, which allows compiling all the work of analysis and design. The obtained results show the strengths and weaknesses of the application for the secure distribution of a quantum final key. Although this work is primarily the development of the implementation that simulates the behavior of the E91 protocol, it is essentially demonstrative.

Keywords: Quantum mechanics, quantum cryptography, quantum protocol E91, E91 simulator, distributed programming, RMI.

[1] Escuela Universitaria de Ingeniería Industrial, Informática y Sistemas. Universidad de Tarapacá. 18 de septiembre 2222. Arica, Chile. E-mail: lcaceres@uta.cl; roberto.fritis@gmail.com; patricio.collao@alumnos.uta.cl

INTRODUCCIÓN

Debido al explosivo aumento en el intercambio de información a través de Internet en la sociedad moderna, la seguridad y privacidad en las comunicaciones se convierten en una de las áreas tecnológicas de desarrollo con mayor importancia en la actualidad. En la informática este desarrollo se refleja en la evolución de los sistemas criptográficos.

La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo personas autorizadas puedan entender el mensaje. La criptografía clásica se divide en dos grandes ramas, la criptografía de clave secreta o simétrica y la criptografía de clave pública o asimétrica. Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo [1].

Mientras que la mayoría de las tecnologías criptográficas actuales, tales como *RSA*[2], *DES*[3], *ECC*[4] y otros tienen sus bases en la factorización de números primos de gran tamaño, en los logaritmos discretos y otras operaciones exponenciales matemáticas, el algoritmo de Shor [2] en un computador cuántico puede resolver eficazmente los problemas de ecuaciones exponenciales. Por lo tanto los sistemas criptográficos actualmente disponibles se volverán inútiles y carentes de seguridad [3-4] cuando los computadores cuánticos se vuelvan una realidad.

Con el fin de hacerle frente a este nuevo tipo de computación, cuyas velocidades de cálculo son potencialmente mucho mayores a las que se ofrecen con la computación actual, se investiga el desarrollo de un nuevo tipo de sistema criptográfico, la denominada Criptografía Cuántica. Aquí la seguridad de las comunicaciones está garantizada por un grupo de teoremas y principios basados en la Mecánica Cuántica especialmente por el principio de incertidumbre, el principio de superposición y el principio de entrelazamiento cuántico, lo que la hace virtualmente irrompible y capaz de detectar de manera temprana en la comunicación la presencia de usuarios no autorizados.

El objetivo del presente trabajo, es el desarrollar una aplicación multiplataforma que sea capaz de simular el funcionamiento del protocolo de criptografía cuántica E91, protocolo desarrollado en base a uno de los más importantes principios de la mecánica cuántica, el denominado entrelazamiento cuántico. La motivación que lleva al desarrollo de este simulador, es el de entregar una herramienta de carácter demostrativa que permita ayudar a entender el proceso de generación de una llave cuántica segura utilizando el protocolo E91, a usuarios que no tengan una base o conocimiento profundo de la mecánica cuántica. Para lograr dicho objetivo se realiza un estudio y análisis profundo de los principios y leyes más importantes de la mecánica cuántica, y sus derivados que son la computación cuántica y la criptografía cuántica.

IMPORTANCIA DE LA CRIPTOGRAFÍA CUÁNTICA

La criptografía cuántica es una de las áreas más recientes en investigación dentro de la criptografía, está basada en los principios de la mecánica cuántica para transmitir y proteger la información, de manera que solo pueda ser accedida por los usuarios autorizados. Su desarrollo surge de la investigación de la computación cuántica como un medio a futuro para proteger la información de manera que esta continúe siendo segura y su transmisión sea más confiable y privada.

La seguridad de los sistemas criptográficos cuánticos radica en la distribución de las claves (Figura 1). Un cambio en el estado cuántico del sistema ocurre cuando un intruso captura los bits cuánticos utilizados para la generación de la clave de comunicación. El intruso, entonces, puede ser detectado debido a la modificación que sufre el estado cuántico del sistema. Por lo tanto, el estudio y desarrollo de la criptología cuántica está enfocada a la investigación de un Protocolo de Distribución de Clave Cuántica

[2] RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente [24].

[3] DES (Data Encryption Standard, estándar de cifrado de datos) es un algoritmo desarrollado originalmente por IBM en la década de los 70 a requerimiento del NBS (National Bureau of Standards, Oficina Nacional de Estandarización) [27].

[4] ECC (Elliptic curve cryptography, Criptografía de Curva Elíptica) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas [28] .

(QKD)[5] que sea práctico y eficiente [5]. Además, recientemente se ha convertido en un tema importante de investigación en la mecánica cuántica.

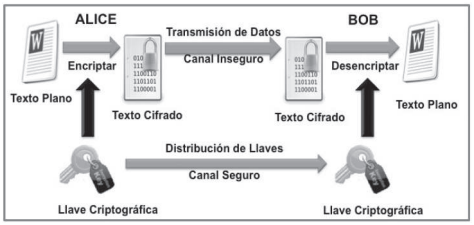

Figura 1. Modelo de comunicación y transmisión de mensajes privados por un canal inseguro (Fuente: basado en [6]).

Una de las mayores ventajas de la criptografía cuántica, es su capacidad de detectar los intrusos y las intercepciones en el canal. El estado del sistema cuántico cambia cuando una intercepción o escucha en las comunicaciones es detectada. Por consiguiente solamente los usuarios autorizados del sistema pueden descubrir que el estado cuántico del sistema ha cambiado, mientras que un espía no puede determinar el estado cuántico del sistema ni duplicarlo, por los principios fundamentales de la mecánica cuántica. Los sistemas criptográficos pueden lograr una seguridad incondicional, y de esta manera garantizar una comunicación segura [7].

La gran desventaja que existe en los proyectos de investigación relacionados con la mecánica cuántica, como por ejemplo la criptografía cuántica y la computación cuántica, son sus altos costos y es allí de la necesidad de utilizar otras herramientas que ayuden en la comprensión y estudio de la criptografía cuántica, en este caso a través del desarrollo de un simulador.

CONCEPTOS PRELIMINARES DE LA MECÁNICA CUÁNTICA PARA EL DESARROLLO DEL PROTOCOLO E91

Sabemos que la codificación usando claves secretas aleatorias de un solo uso (*one time pad*) [8] permite llevar a cabo una comunicación segura, pero presenta la dificultad práctica de la distribución segura de las claves. Afortunadamente, las leyes de la mecánica cuántica proporcionan herramientas para abordar el problema de la distribución segura de claves secretas. La contribución cuántica a la seguridad del proceso consiste esencialmente en que un espía no puede extraer información sin revelar su presencia a los comunicantes, ya que por las leyes de la mecánica cuántica no es posible copiar estados.

Existen diversos protocolos para la distribución cuántica de claves secretas. En un proceso de distribución cuántica de claves, intervienen un emisor y un receptor y dos canales de comunicación (ver Figura 2), uno cuántico para enviar fotones u otras partículas subatómicas y otro clásico y posiblemente público para reconciliar y depurar la información. Los dos comunicantes usan un trozo de su clave para detectar la presencia de espías. Un posible espía puede acceder al canal clásico, y también puede acceder al canal cuántico y usar todos los medios que desee con la única restricción de que sean compatibles con las leyes de la mecánica cuántica [9].

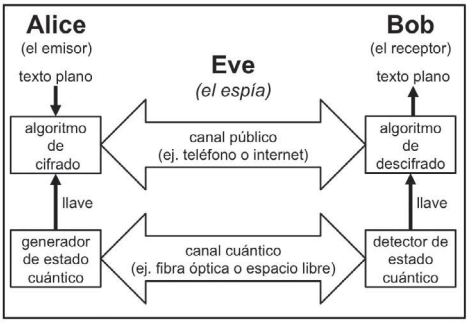

Figura 2. Modelo de Comunicación Cuántica (Fuente: basado en [10]).

A continuación se aborda el protocolo de comunicación cuántica E91, para su análisis y posterior implementación a través de una simulación. Para ello se comienza con un breve análisis de los trabajos que permitieron la creación y el desarrollo de este protocolo. Bajo este punto de vista, a continuación se discute sobre los conceptos más importantes para entender el funcionamiento de la criptografía cuántica pero sobre todo aquellos conceptos que dan vida al protocolo creado por Artur Ekert [11].

Paradoja EPR - Einstein, Podolsky y Rosen

Un experimento mental realizado por Einstein, Podolsky y Rosen, en 1935 [12], explica la base

[5] Quantum key distribution (QKD) utiliza las propiedades de la mecánica cuántica para garantizar una comunicación segura. Permite que dos partes produzcan una clave secreta común aleatoria conocida sólo por ellos, que luego se pueda utilizar para cifrar y descifrar los mensajes [29].

conceptual del porqué la criptografía cuántica funciona. Nombrada la paradoja EPR, en un principio se diseñó para demostrar que la mecánica cuántica no es una teoría física completa, pero rápidamente se convirtió en un ejemplo de cómo la mecánica cuántica desafía la intuición clásica. El trío EPR se basó en los principios clásicos como localidad y realismo. El principio de localidad establece que los objetos distantes no pueden tener una influencia directa una sobre otra. Esta suposición implica que el resultado de una medición realizada en un objeto no puede influir en las propiedades de otro objeto. El realismo es la idea de que existe una realidad que es independiente del observador, e implica que los objetos tienen propiedades definidas que no son afectados por diferentes tipos de mediciones realizadas en ellos. Estas dos condiciones aparentemente razonables son violadas en el ámbito de la criptografía cuántica [11].

Teorema de Bell

El físico John S. Bell demostró que lo que Einstein y sus colegas tomaron como paradoja podía demostrarse científicamente. El teorema de Bell prueba la conexión-correlación entre sistemas no relacionados causalmente. Bell comenzó a estudiar el problema de la no localidad y, en particular, la cuestión de si la misma es un requisito necesario para que una teoría de variables ocultas sea consistente con todas las predicciones cuánticas. El Teorema de Bell, publicado en 1965, da una respuesta afirmativa a esta interrogante: "*toda teoría de variables ocultas que sea determinista y local tiene necesariamente algunas predicciones incompatibles con la Mecánica Cuántica*" [13]. Este resultado implica que las teorías deterministas locales de variables ocultas y la Mecánica Cuántica son mutuamente excluyentes [14].

Los Protocolos QKD basados en las Desigualdades de Bell

Los protocolos de distribución de claves más recientes se basan en el teorema de Bell [5, 15]. Estos protocolos transmiten las partículas entrelazadas entre un emisor y un receptor, permitiendo a ambos comparar abiertamente sus partículas recibidas y verificar si sus estados cuánticos violan la desigualdad de Bell. Si el grado de violación no es el anticipado, eso significa que el estado cuántico interno ha sido alterado, y la probabilidad de que estén siendo espiados es extremadamente alta. De esta manera se puede confirmar una comunicación segura y los intrusos ser detectados [9, 16].

Protocolo E91

Este protocolo criptográfico fue desarrollado por Artur Ekert en 1991 [11] y se encuentra basado en el Teorema de Bell [13]. El protocolo E91 utiliza fotones entrelazados. Estos pueden ser preparados por Alice, Bob o algún tercero, y son distribuidos de manera que Alice y Bob tengan un fotón de cada par. El modelo se fundamenta en propiedades del entrelazamiento cuántico.

A pesar de que muchas cantidades físicas (observables) pueden ser utilizadas para explicar la creación del entrelazamiento cuántico, Ekert utiliza los estados cuánticos llamados singlet de spin [17].

El entrelazamiento cuántico es la incapacidad para definir el estado cuántico de un objeto sin referenciar al estado cuántico de otro objeto, el cual puede estar o no, alejado espacialmente del primero. Aunque no se pueden establecer conclusiones acerca de los estados individuales de los objetos, el estado cuántico de ambos objetos está bien definido [18].

A continuación se detalla paso a paso el funcionamiento del protocolo de acuerdo al trabajo original de 1991, según [11] y [18], el siguiente pseudocódigo detalla el proceso completo de generación e intercambio de claves:

1. Alice le indica a la fuente la longitud de la clave.
2. La fuente crea todos los pares entrelazados.
3. La fuente comienza el envío de partículas entrelazadas en paralelo hacia Alice y Bob (ver Figura 3).
4. A medida que van llegando las partículas entrelazadas, Alice y Bob generan una base de forma aleatoria e independiente entre ellos.
5. Una vez terminado el envío de los pares entrelazados desde la fuente a Alice y a Bob, la fuente le envía una señal a Alice y a Bob comunicándole el hecho.
6. Una vez recibida la señal por parte de la fuente, Alice y Bob comienzan el intercambio de sus respectivas bases.
7. Cuando finaliza el envío de las bases de ambos participantes, Alice y Bob se disponen a comparar sus propias bases con las bases del otro.

8. Se forman 2 grupos de datos, el primer grupo corresponde a aquellos donde se detectan bases contrarias y el segundo grupo aquellas en que se utilizan las mismas bases.
9. El primer grupo es descartado, ya que para efecto de esta simulación no es necesario su utilización.
10. El segundo grupo, las cuales corresponde a aquellas donde Alice y Bob utilizaron las mismas bases, su anti correlación está demostrada, así que se dispone a la medición de las partículas entrelazadas que se encuentra almacenada en la misma posición que la base (por parte de Alice y de Bob).
11. Las medidas obtenidas se pueden convertir en una cadena secreta de bits o sea la clave. Está clave secreta puede entonces ser utilizada en una comunicación criptográfica convencional entre Alice y Bob.

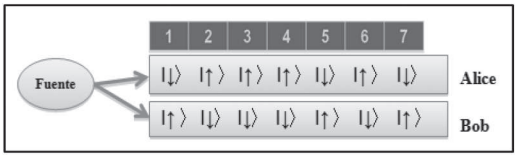

Figura 3. Modelo de transmisión de Partículas en el protocolo E91.

En la Figura 4 se muestra un ejemplo gráfico del intercambio de bases y de coincidencias para el establecimiento de una QKD entre Alice y Bob.

Para detectar si Eve (intruso) ha estado espiando en la comunicación, Alice y Bob comparan las claves rechazadas (primer grupo que corresponden a aquellos donde se detectan bases contrarias). Debido al hecho de que Eve tiene que realizar una medición sobre una de las partículas del par entrelazado para poder leer la información pertinente a la comunicación, ella rompe las propiedades propias del entrelazamiento y luego al comprobar la presencia de intrusos utilizando las desigualdad de Bell [19], se produce la detección de Eve en la comunicación, de manera oportuna.

SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN CUÁNTICA E91

Para este trabajo, se selecciona el protocolo E91 [11], el cual utiliza algunos principios de la mecánica cuántica, que no son utilizados por los protocolos BB84 [20] (implementado en [21] y mejorado en [22]) y B92 [23], para establecer una comunicación segura entre los participantes autorizados en la comunicación. El protocolo E91 utiliza un principio emblemático de la mecánica cuántica, como lo es el entrelazamiento cuántico, cuya utilización permite una mayor probabilidad en la detección de intrusos o espías durante la comunicación, a diferencia de los otros protocolos, como el desarrollo en el simulador BB84 [22], siendo que utilizando las mismas tecnologías y estructuras de software, el simulador BB84 no representa el entrelazamiento cuántico, pues el protocolo mismo no lo utiliza.

	Medición 1	**Medición 2**	**Medición 3**	**Medición 4**	**Medición 5**	**Medición 6**
Esquema de Alice[6]	⊕	⊘	⊖	⊕	⊕	⊘
Partículas de Alice	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$
Esquema de Bob[6]	⊕	⊘	⊘	⊘	⊕	⊘
Partículas de Bob	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$	$\|\downarrow\rangle$	$\|\downarrow\rangle$	$\|\uparrow\rangle$
Coincidencias en las Bases	✓	✗	✗	✗	✓	✓
Clave	0				1	0

Figura 4. Ejemplo de Comunicación del Protocolo E91.

[6] Esquema de Alice y Bob son el conjunto de bases utilizadas por Alice y Bob respectivamente, para medir las partículas entrelazadas que son enviadas por la Fuente. Las bases utilizadas para dicha medición están especificadas en el trabajo [11].

Requerimientos de la Aplicación E91
Los requerimientos necesarios para la aplicación, son una descripción de las necesidades que esta necesita satisfacer. El objetivo principal en esta etapa es identificar qué es lo que en realidad se necesita cumplir para un óptimo desempeño de la aplicación.

Requerimientos Funcionales
Definen las funciones que el sistema será capaz de realizar y cómo se tendrá que comportar el sistema durante su ejecución. A continuación las identificamos:

- Generar la secuencia de partículas entrelazadas que será transmitida.
- Generar el esquema que será utilizado para medir las partículas.
- Permitir transmitir la secuencia de partículas entrelazadas por algún canal de comunicación.
- Permitir medir las partículas entrelazadas con las bases almacenadas en el esquema.
- Permitir transmitir el esquema por algún canal de comunicación.
- Permitir comparar los esquemas utilizados entre los usuarios.
- El sistema deberá poder funcionar de forma distribuida.

En la Figura 5 se exhibe un diagrama general de los proceso de intercambios de mensajes que suceden dentro del simulador del protocolo E91.

Este diagrama fue desarrollado para entender de manera general el funcionamiento del protocolo y de esta manera trazar los requerimientos funcionales que serán necesarios. El análisis del diagrama nos muestra cómo se realizan los intercambios de mensajes entre los distintos participantes dentro de la comunicación, en primer lugar la Fuente, es la encargada de enviar las partículas entrelazadas que son generadas por ella, hacia los usuarios (Alice y Bob).

Posteriormente Alice y Bob intercambiarán los esquemas propios de cada uno, que fueron producidos a partir de las bases que utilizaron para medir las partículas enviadas por la Fuente. Una vez que se comparten los esquemas, se comparan y a partir de los resultados se logra generar una clave final secreta que se utilizará con un sistema de cifrado clásico simétrico para cifrar el mensaje y transmitirlo por un canal clásico inseguro.

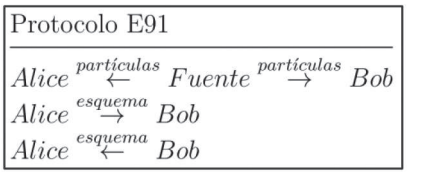

Figura 5. Diagrama general de intercambio de mensajes dentro del simulador E91.

DESARROLLO DE LA APLICACIÓN

Arquitectura y lenguaje usado en la Aplicación
La arquitectura que tendrá la aplicación, será la de un modelo cliente/servidor adaptada para nuestros requerimientos y se usará la tecnología de Java RMI para la comunicación distribuida. Por lo tanto, por estas y otras características que lo hacen un lenguaje robusto, se elige a Java como el lenguaje de programación a utilizar en la aplicación y Netbeans[7] como la plataforma de trabajo.

El motivo para la utilización del Middleware[8] Java RMI fue principalmente debido a que el desarrollo del simulador del protocolo BB84 [22] fue realizado mediante la utilización de la misma tecnología. Por tanto, para este trabajo también se optó por la utilización del mismo middleware, lo cual permitirá realizar en trabajos posteriores, comparaciones entre ambos simuladores, utilizando ambientes de pruebas similares.

Sin embargo, debemos especificar la influencia en el comportamiento del desempeño del sistema, en el sentido de que por cada partícula enviada, se crea una conexión RMI, lo que puede provocar un retardo constante en el tiempo en cada caso de prueba realizado.

Definiciones Previas
Como primer paso procedemos a definir algunos conceptos previos que se usaran en la especificación del modelamiento de la aplicación.

[7] NetBeans es un entorno de desarrollo integrado open-source, hecho principalmente para el lenguaje de programación Java que permite que las aplicaciones sean desarrolladas a partir de un conjunto de componentes de software llamados módulos [25].

[8] Middleware es la capa de software intermedio entre el cliente y el servidor, representa el software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, redes, hardware y/o sistema operativo [30].

De acuerdo al conjunto de pasos definidos anteriormente en el pseudocódigo desarrollado, procederemos primero a definir los siguientes conceptos esenciales para la construcción de la aplicación:

- ***Clave Final:*** Conjunto de números binarios que son generados por el emisor y el receptor (clave única), una vez que ambos han compartido y medido sus respectivos esquemas junto con las partículas recibidas. Por ejemplo, la siguiente sería una secuencia válida:

  01011010011…1

- ***Esquema*****:** Es un conjunto de símbolos representativos de las bases elegidas para cifrar los datos. Las bases que se utilizan son caracterizadas por los ángulos azimutales[9]:

$$\varnothing_1^a = 0°, \varnothing_2^a = 45°, \varnothing_3^a = 90°, \text{ y}$$
$$\varnothing_1^b = 45°, \varnothing_2^b = 90°, \varnothing_3^b = 135°$$

- ***Ejemplo de esquemas*****:** Sean las bases que puede tomar Alice = (–), (/), (|) y las bases que puede tomar Bob = (/), (|), (\). Entonces un esquema válido de bases generadas aleatoriamente sería el siguiente:

  (–) (|) (|) (/) (–) (|) (/) (|) (/)……(–)

- ***Partículas Entrelazadas****:* Conjunto de símbolos que representan la propiedad de la mecánica cuántica, denominado entrelazamiento cuántico. La fuente genera un par de partículas entrelazadas, representadas mediante los símbolos $|\uparrow\rangle$ y $|\downarrow\rangle$ que corresponden a los valores +1 (spin hacia arriba) y -1 (spin hacia abajo), de cada partícula. De esta forma una secuencia válida de partículas entrelazadas sería la siguiente:

  $|\uparrow\rangle\,|\downarrow\rangle$ - $|\downarrow\rangle\,|\uparrow\rangle$ - $|\uparrow\rangle\,|\downarrow\rangle$ - $|\downarrow\rangle\,|\uparrow\rangle$ - $|\uparrow\rangle\,|\downarrow\rangle$ - $|\uparrow\rangle\,|\downarrow\rangle$ - $|\downarrow\rangle\,|\uparrow\rangle$ ..... $|\downarrow\rangle\,|\uparrow\rangle$

[9] El ángulo azimutal es el ángulo con respecto al norte geográfico. Este ángulo es igual a cero hacia el norte, 90° hacia el este, 180° hacia el sur y 270° hacia el oeste [26].

Implementación de la Aplicación E91

En esta sección se muestra la implementación del simulador criptográfico cuántico E91, que en su etapa inicial de pruebas se desarrolló para ser ejecutada de manera local y luego extender su funcionalidad a un ambiente distribuido, una vez que se encuentre funcionando correctamente la aplicación, se evalúa su comportamiento mediante pruebas que permitirá medir su desempeño en una situación simulada de la realidad, con lo cual se culmina la implementación de la aplicación.

Configuraciones previas y puesta en marcha

Para las pruebas que se realizarán, se utilizó la aplicación primero de manera local, donde los 2 participantes de la comunicación (Alice y Bob) y la Fuente se ejecutan en un solo equipo (ver Figura 6). Posteriormente se realizarán las pruebas de manera distribuida, donde cada elemento dentro de la aplicación es ejecutado en distintos equipos y con distintos sistemas operativos (ver Figura 7).

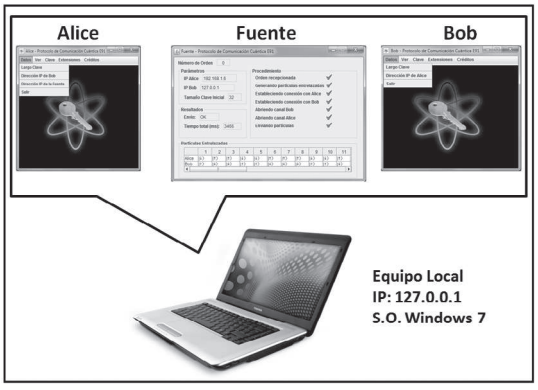

Figura 6. Ejecución de la aplicación de manera local.

En la Figura 8 (a-d), se muestran los pasos realizados en la configuración de los equipos Alice (máquina 1) y Bob (máquina 2).

En la aplicación Alice se selecciona "*Iniciar generación*" en el menú "*Clave*", el cual una vez se hayan ingresado todos los parámetros anteriores para la comunicación, dará inicio al proceso de generación de una clave cuántica.

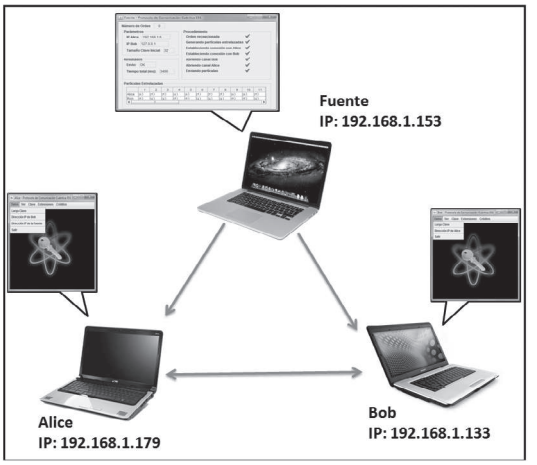

Figura 7. Ejecución de la aplicación de manera distribuida.

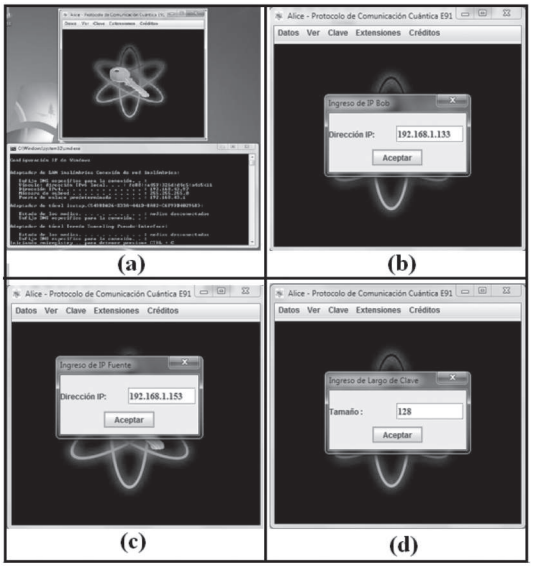

Figura 8. Configuración del receptor en el simulador cuántico E91.

a. Alice y Bob abren su sesión. En la parte inferior se inició rmiregistry por consola, mostrando también la IP del mismo.
b. Se ingresa la dirección IP de Bob (solo válido para Alice). En caso de la aplicación Bob debe ingresarse la dirección IP de Alice.
c. Se ingresa la dirección IP de la Fuente (solo válido para Alice).
d. Se ingresa el tamaño inicial de la clave a establecer (válido para Alice y para Bob).

Proceso de Comunicación Segura del Simulador

En esta etapa se establece la comunicación segura entre Alice y Bob, una vez realizada la configuración previa de ambos equipos (como se muestra en la sección anterior) y haber puesto en marcha la aplicación Fuente.

La Fuente al ser ejecutada, despliega una ventana como la que se ve en la Figura 9, esta aplicación no posee ingreso de datos por parte del usuario, toda la información que ella necesita es enviada por Alice, una vez que esta última solicita establecer la comunicación con los demás elementos participantes de la comunicación. La información desplegada en la fuente tiene relación con los parámetros de comunicación establecidos, el orden de las partículas entrelazadas generadas y enviadas por el canal de comunicación y un conjunto de procedimientos que se van marcando conforme estos se van cumpliendo.

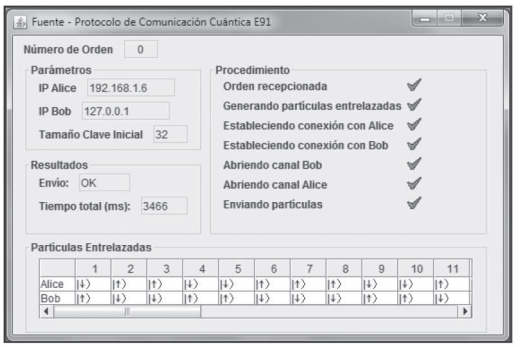

Figura 9. Interfaz gráfica de la Fuente.

Las aplicaciones Alice y Bob por su parte también tienen la capacidad de desplegar por pantalla los resultados obtenidos al finalizar la comunicación, para ello se utilizan ventanas que muestran por pantalla el cifrado de datos (ver Figura 10), junto a toda la información obtenida durante el proceso de generación de la clave final cuántica. Finalmente se muestra cuál es la clave final en común, obtenida por ambos usuarios y otros datos que son generados a partir de esta clave.

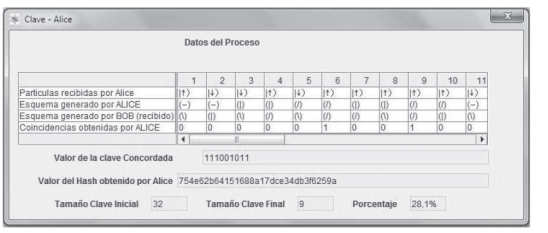

Figura 10. Ventana de cifrado de la aplicación.

Una vez generada y compartida la clave cuántica, podemos proceder a cifrar los datos con ésta, para

ello se selecciona la opción "*Enviar mensaje cifrado*" que se encuentra en el menú "*Extensiones*" (válido solo para Alice), el cual desplegara una ventana como el de la Figura 11.

Donde podemos ingresar una palabra o frase cualquiera, que será cifrada de acuerdo a un algoritmo de criptografía simétrica (AES) y la clave final obtenida.

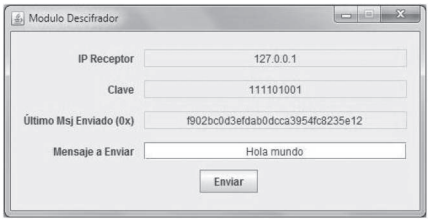

Figura 11. Ventana de cifrado de la aplicación Alice.

Para poder ver el mensaje recibido desde la aplicación Bob se debe seleccionar la opción "*Ver mensaje recibido*" que se encuentra en el menú "*Extensiones*" (válido solo para Bob), el cual desplegará una ventana como el de la Figura 12.

En dicha ventana se puede ver el resultado del cifrado por parte del algoritmo AES y la clave cuántica compartida. Cabe señalar que para cualquiera de los participantes en esta comunicación, el resultado del cifrado será el mismo.

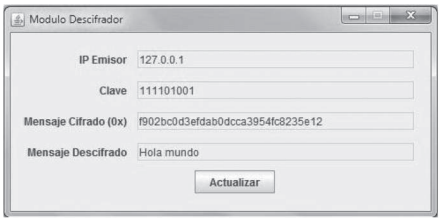

Figura 12. Ventana de cifrado de la máquina Bob.

ANÁLISIS Y PRUEBAS DE LA APLICACIÓN

En esta sección se describirán las pruebas correspondientes a la aplicación. En primer lugar, se definirán los requerimientos necesarios de cada prueba para ejecutar la aplicación. En seguida, se procede al testeo de la aplicación con diferentes valores de entradas, lo cual permitirá obtener claves finales que serán utilizados para cifrar y descifrar mensajes con algoritmos tradicionales simétricos.

Pruebas de la Aplicación

Para realizar estas pruebas se utilizaron distintas clases de computadores, con sus respectivos sistemas operativos instalados (Windows, Mac OS) y los cuales se encuentran en diferentes redes. Para estas pruebas se utilizó la Tabla 1, en la cual se tienen los largos comunes para las claves que se usan en criptografía simétrica.

Tabla 1. Largo de Claves.

Largo de Claves		
8 bits	64 bits	512 bits
16 bits	128 bits	1.024 bits
32 bits	256 bits	2.048 bits

Caso de Prueba 1

Para la primera prueba se conectan los 3 computadores dentro de una misma red local, esto por medio de un router WIFI cuya puerta de enlace es la dirección IP 192.168.1.5. Para tal efecto se diseñó el diagrama de Red que se muestra en la Figura 13, por medio de esta conexión se puede realizar una comunicación exitosa entre los distintos equipos. La configuración que se utiliza para cada computador en esta prueba se muestra de forma detallada en la Tabla 2.

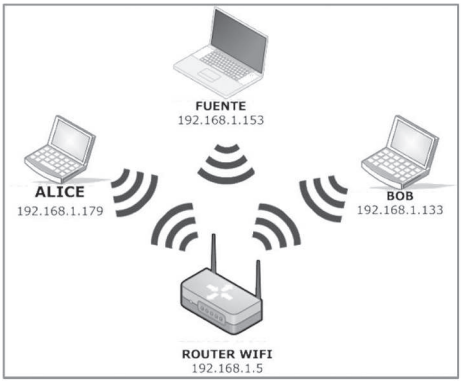

Figura 13. Diagrama de red para la prueba 1.

Tabla 2. Configuración equipos para prueba 1.

Prueba 1. Una red local WIFI			
Usuarios	**Dirección IP**	**Máscara de subred**	**Puerta de enlace**
Alice Equipo 1	192.168.1.179	255.255.255.0	192.168.1.5
Bob Equipo 2	192.168.1.133	255.255.255.0	192.168.1.5
Fuente Equipo 3	192.168.1.153	255.255.255.0	192.168.1.5

A continuación en la Tabla 3, se detallan los resultados obtenidos en las pruebas, es importante señalar que dichos resultados son la ponderación o promedio de las 3 pruebas que se realizaron por cada largo de clave o bits iniciales.

Tabla 3. Resultados de la prueba 1 de la Aplicación.

Nº Bits Iniciales	Nº Bits Finales	Tiempo Total (seg.)	Bits Perdidos
8	1,7	5,3	6,3
16	3,7	7,3	12,3
32	9,0	11,2	23,0
64	15,3	22,2	48,7
128	27,0	41,3	101,0
256	58,0	84,9	198,0
512	114,0	171,8	398,0
1.024	233,7	341,4	790,3
2.048	443,3	726,4	1604,7

En la Figura 14 se observa gráficamente cómo varían las porciones de bits finales de cada prueba, donde el largo de la clave final siempre variará entre el 20% y el 30% del tamaño inicial de la clave, lo que se explica, ya que la probabilidad de que Alice y Bob escojan bases compatibles para medir las partículas entrantes es de $\frac{1}{3}$ tal como se explica en [18]. Por tal motivo, como solo se ocuparán para la clave, aquellos bits que fueron detectados cuando Alice y Bob utilizaron bases compatibles, entonces este proceso de filtrado puede disminuir el tamaño de la clave hasta un 30% de su tamaño original.

Finalmente luego de un análisis de los resultados que se obtuvieron para el caso de prueba 1, se concluye que a medida que aumenta el número de bits iniciales en la simulación, el tiempo de respuesta utilizado por el sistema para generar la clave final también se incrementa progresivamente y el número de bits finales que corresponden a la clave final obtenida, tendrá un tamaño que rondará $\frac{1}{4}$ del tamaño inicial de bits.

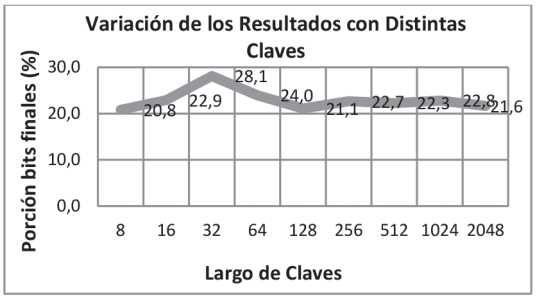

Figura 14. Promedio de variación de la clave final versus los distintos largos de clave inicial.

Caso de Prueba 2

En esta segunda prueba se conectan los 3 computadores dentro de una misma red local, pero esta vez la comunicación entre los equipos es por medio de un switch que se conecta a los 3 computadores por medio de un cable de red. Para tal efecto se diseñó el diagrama de Red que se muestra en la Figura 15, por medio de esta conexión se puede realizar una comunicación distribuida entre los distintos equipos, permitiendo que Alice y Bob puedan generar una clave exitosa con el simulador a través de la utilización de la información distribuida en el canal de comunicación.

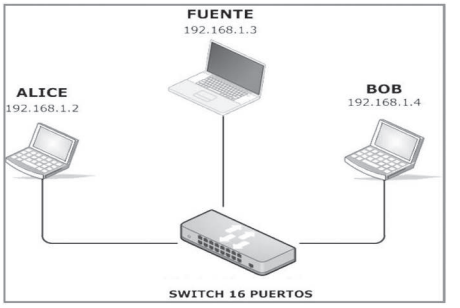

Figura 15. Diagrama de red de la prueba 2.

La configuración de cada computador de esta prueba se encuentra detallada en la Tabla 4.

Tabla 4. Configuración equipos para prueba 2.

Prueba 2. Una red local cableada		
Usuarios	**Dirección IP**	**Máscara de subred**
Alice (Equipo 1)	192.168.1.2	255.255.255.0
Bob (Equipo 2)	192.168.1.4	255.255.255.0
Fuente (Equipo 3)	192.168.1.3	255.255.255.0

A continuación en la Tabla 5, se detallan los resultados que se obtuvieron en las pruebas.

Es importante señalar que los resultados obtenidos en la prueba 2, son la ponderación o promedio de las 3 pruebas que se realizaron por cada largo de clave o bits iniciales.

A continuación en la Figura 16 se muestra gráficamente como varían los resultados obtenidos

Tabla 5. Resultados de la prueba 2 de la Aplicación.

Nº Bits Iniciales	Nº Bits Finales	Tiempo Total (seg.)	Bits Perdidos
8	1,0	2,5	7,0
16	2,7	4,9	13,3
32	5,3	9,8	26,7
64	14,0	19,5	50,0
128	29,0	38,8	99,0
256	59,3	79,0	196,7
512	111,0	155,5	401,0
1024	229,0	310,4	795,0
2048	462,0	619,4	1586,0

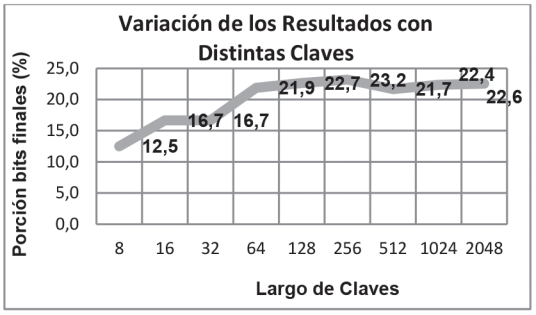

Figura 16. Promedio de variación de la clave final versus los distintos largos de clave inicial.

para cada largo de clave inicial, donde la porción de bits finales es obtenida a partir del promedio de todas las pruebas hechas para cada bit inicial. Se puede observar que al contrario de la prueba anterior que se realizó en un medio inalámbrico y que la clave siempre variaba entre el 20% y el 30%. En esta prueba en cambio se utilizaron cables de red para la comunicación la cual posee menos perdida de señal o interferencias que un medio inalámbrico sobre todo para distancias pequeñas. Lo cual por ende producía una variación incremental en los resultados obtenidos con distintas claves, el gráfico enseña que los bits finales tuvieron una variación entre un 10% y un 25%, o sea mientras menor es el número de bits iniciales, menor va a ser el número de bits finales, pero siempre manteniendo un límite para el largo de la clave final en un 30% del tamaño inicial de la clave, lo que se explica, ya que la probabilidad de que Alice y Bob escojan bases compatibles para medir las partículas entrantes es de $\frac{1}{3}$ tal como se explica en [18].

Finalmente, luego de un análisis de los resultados obtenidos para el caso de prueba 2, se concluye que a medida que aumenta el número de bits iniciales en la simulación, el tiempo de respuesta utilizado por el sistema también se incrementa progresivamente y el número de bits finales que corresponden a nuestra clave, mantendrá un aumento entre cada prueba correspondiente al doble del resultado de la clave final anterior. En este caso el tiempo de ejecución de la aplicación para cada clave inicial es notablemente menor que el tiempo utilizado en un medio inalámbrico (wifi), sin embargo, la diferencia en el largo de la clave final entre ambos casos de prueba son similares.

Caso de Prueba 3

Para la prueba número 3, cada computador se conecta a una red distinta, lo que significa que existirán 3 subredes individuales distintas conectadas mediante los routers 1, 2 y 3, los cuales a su vez se encuentran unidas por medio de un switch de 16 puertos y una velocidad de 10/100 Mbps de transferencia. Para tal efecto se diseñó el diagrama de Red que se muestra en la Figura 17, por medio de esta conexión se puede realizar una comunicación distribuida entre los distintos equipos, lo que permite que Alice y Bob puedan generar una clave exitosa con el simulador.

La configuración de cada computador de esta prueba se encuentra detallada en la Tabla 6. A continuación en la Tabla 7, se detallan los resultados obtenidos en las pruebas, es importante señalar que dichos resultados son la ponderación o promedio de las 3 pruebas que se realizaron por cada largo de clave o bits iniciales.

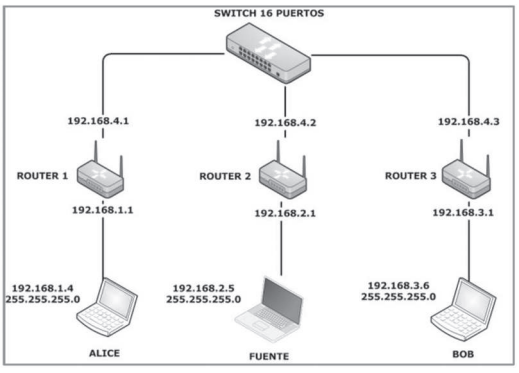

Figura 17. Diagrama de red de la prueba 3.

Tabla 6. Configuración equipos para prueba 3.

Prueba 3. Una red local cableada			
Usuarios	**Dirección IP**	**Máscara de subred**	**Puerta de enlace**
Alice Equipo 1	192.168.1.4	255.255.255.0	192.168.1.1
Bob Equipo 2	192.168.3.6	255.255.255.0	192.168.3.1
Fuente Equipo 3	192.168.2.5	255.255.255.0	192.168.2.1

En la Figura 18 se puede observar gráficamente como varían los resultados obtenidos para cada largo de clave inicial, donde la porción de bits finales es obtenida a partir del promedio de todas las pruebas hechas para cada bit inicial. Entre los 8 bits y los 64 bits iniciales para cada prueba, existe un incremento sustancial en el largo de la clave final obtenida, sin embargo a partir de allí, las medidas posteriores mantendrán un promedio constante en el largo de claves finales entre los 22% y los 23% del tamaño de bits iniciales.

Al igual que los casos de pruebas anteriores, se mantiene un límite en el largo de clave final en un 30% del tamaño inicial de la clave, es decir que ninguna clave final que se obtenga en las pruebas superara este valor, lo que se explica, ya que la probabilidad de que Alice y Bob escojan bases compatibles para medir las partículas entrantes es de $\frac{1}{3}$.

Tabla 7. Resultados de la prueba 3 de la Aplicación.

Nº Bits Iniciales	Nº Bits Finales	Tiempo Total (seg.)	Bits Perdidos
8	1,3	2,7	6,7
16	4,3	6,1	11,7
32	7,7	11,0	24,3
64	14,3	19,8	49,7
128	30,3	41,5	97,7
256	63,0	79,0	193,0
512	112,0	157,9	400,0
1024	224,7	315,4	799,3
2048	453,3	630,8	1594,7

Finalmente en la Figura 19, se puede observar que las mediciones realizadas durante el comienzo de la aplicación y utilizando tamaños de claves iniciales pequeños, los resultados obtenidos en el tamaño de las claves finales serán considerablemente distintos, pero a partir de las pruebas donde utilizamos una clave inicial de 64 bits y mayores, entonces el tamaño

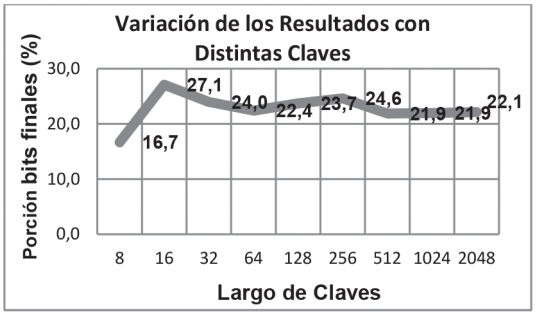

Figura 18. Promedio de variación de la clave final versus los distintos largos de clave inicial.

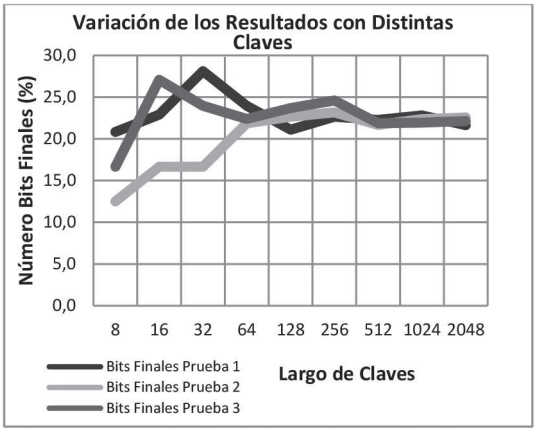

Figura 19. Comparación entre las claves finales e iniciales, obtenidas por los tres casos de pruebas.

final de las claves que se obtendrán para los distintos casos de prueba serán de una longitud similar.

Si bien el tamaño de las claves finales, mantenían una homogeneidad entre los distintos casos de pruebas donde se utilizaban una arquitectura de red y un medio de comunicación distintos. Pero esta homogeneidad se lograba cuando se utilizaban claves iniciales de un tamaño mayor a los 64 bits. Ahora bien esta similitud que se logra en los tamaños de las claves, no se cumple cuando medimos el tiempo de ejecución de los 3 casos de prueba, tal como se muestra en la Figura 20.

Aquí se puede observar que al utilizar como medio de comunicación entre los distintos elementos un cable de red, entonces se logrará un mejor desempeño en la comunicación, que al utilizar un medio inalámbrico para la transmisión de datos. Esta diferencia en el tiempo de ejecución del sistema se

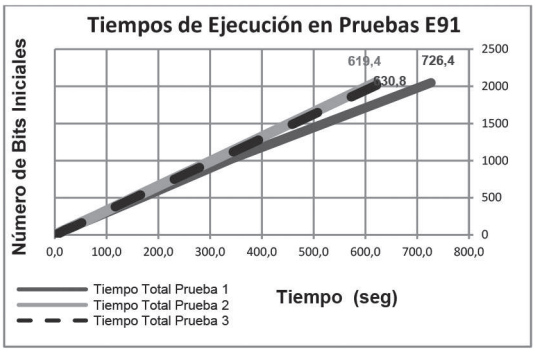

Figura 20. Comparación en el tiempo de ejecución total entre cada prueba.

irá incrementando cada vez más a medida que vaya aumentando el tamaño de las claves iniciales, y esta diferencia en los tiempos de ejecución, se debe a que los cables de red poseen una mayor tolerancia a fallos y una menor pérdida de datos en comparación con un medio inalámbrico.

CONCLUSIONES

El objetivo principal de este trabajo fue desarrollar una aplicación que logre simular el comportamiento del protocolo E91 pero utilizando computadores clásicos, es por ese motivo que la aplicación desarrollada es puramente demostrativa y de carácter académico, para poder ayudar a explicar cómo sería la utilización del protocolo E91 de criptografía cuántica, de manera distribuida, en futuros computadores cuánticos.

En el estudio de los principios de la criptografía cuántica, muchos conceptos de la mecánica cuántica son necesarios de conocer y comprender para entender la filosofía de la criptografía cuántica por completo.

Después del análisis del modelo de software, las pruebas de la aplicación permitieron analizar el comportamiento de la aplicación con respecto a varios largos de claves comunes a los protocolos de criptografía. Si bien los resultados obtenidos demuestran que usando este protocolo se pierden alrededor de un 70% de los bits, de acuerdo a las especificaciones del protocolo, los restantes bits del largo de la clave inicial se pueden considerar como una clave segura compartida y lo interesante de este protocolo es que esta clave final se obtuvo sin que los usuarios tengan que compartir las partículas que recibieron. Ahora, de los resultados obtenidos se concluye que se comporta mejor con una clave de 128 bits de largo inicial, para lograr como largo final de clave una de aproximadamente 30 bits, con un tiempo de generación sobre los 40 segundos. Por lo tanto mientras mayor sea la clave inicial, también será mayor la clave final que se genere y por consiguiente más segura para el cifrado de datos, el punto negativo, es que también aumenta el tiempo utilizado para generar la clave. Por lo tanto el nivel de seguridad que se desee lograr con esta aplicación dependerá del tiempo que decidan los usuarios ocupar para obtenerla.

REFERENCIAS

[1] H. García Molina. “Avances en Informática y Sistemas Computacionales”. Editorial Tabasco. Primera edición. México. Tomo I. 2006. ISBN: 968-5748-98-5.

[2] P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 125-134. Noviembre de 1994. DOI: 10.1109/SFCS.1994.365700.

[3] D.-H. Shih, H.-S. Chiang and C. David Yen. “Classification methods in the detection of new malicious emails”. Information Sciences. Vol. 172 Nº 1-2, pp. 241-261. 9 de junio de 2005. DOI: 10.1016/j.ins.2004.06.003.

[4] I. Seok Ko, C. Seong Leem, Y. Ji Na and C. Young Yoon. “Distribution of digital contents based on public key considering execution speed and security”. Information Sciences. Vol. 174 Nº 3-4, pp. 237-250. Agosto de 2005. ISSN: 0020-0255.

[5] Y. Fang Chung, Z. Yu Wu and T. Shyong Chen. “Unconditionally secure cryptosystems based on quantum cryptography”. Information Sciences. Vol. 178 Nº 8, pp. 2044-2058. 15 de Abril de 2008. DOI: 10.1016/j.ins.2007.11.013.

[6] A. Shields and Z. Yuan. “Key to the quantum industry”. Physics World, pp. 24-29. Marzo de 2007.

[7] D.G. Mendoza Vázquez. “Introducción a la teoría de la Información Cuántica”. Tesis para obtener el título de Licenciado en Ciencias de la Computación. Universidad Nacional Autónoma de México. México. 2010.

[8] N.R. Wagner. “The Laws of Cryptography with Java Code”, pp. 82-83. 2003. Fecha de consulta: Enero de 2014. URL: http://

www.cs.utsa.edu/~wagner/lawsbookcolor/laws.pdf

[9] A. García López and J. García López. "Criptografía cuántica". Departamento Matemática Aplicada. Escuela Universitaria de Informática. Universidad Politécnica de Madrid. España. 2005.

[10] C. Elliott, D. Pearson and G. Troxel. "Quantum Cryptography in Practice". Cornell University Library, arXiv. Julio de 2003.

[11] A. Ekert. "Quantum cryptography based on Bell's theorem". American Physical Society. Vol. 67 Nº 6, pp. 661-663. Agosto 1991. DOI: 10.1103/PhysRevLett.67.661.

[12] A. Einstein, B. Podolsky and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?". Physical Review. Vol. 47 Nº 10, pp.777-780. 15 de Mayo de 1935. DOI: 10.1103/PhysRev.47.777.

[13] J.S. Bell. "On the Einstein Podolsky Rosen paradox". Physics. Vol. 1. pp. 195-200. 1964.

[14] G. Abal. "Paradoja EPR y desigualdades de Bell: pruebas experimentales, estado actual del conocimiento". Instituto de Física. Universidad de la República. Montevideo, Uruguay. Febrero 2007.

[15] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera. "Quantum privacy amplification and the security of quantum cryptography over noisy channels". Physical Review Letters. Vol. 77 Nº 13, pp. 2818-2821. September, 1996. DOI: 10.1103/PhysRevLett.77.2818.

[16] W.-Y. Hwang. "Bell's inequality, random sequence, and quantum key distribution". Physical Review A. Vol. 71 Nº 5, pp. 52329-52331. May, 2005. DOI: 10.1103/PhysRevA.71.052329.

[17] D.J. Griffiths. "Introduction to Quantum Mechanics". Prentice Hall. New Jersey, Estados Unidos, pp. 166. 1995. ISBN: 0-13-124405-1.

[18] N. Ilic. "The Ekert Protocol". Journal of Phy334. Nº 1. 22 de julio de 2007.

[19] J.S. Bell. "Introduction to the hidden variable question". Proceedings of the International School of Physics 'Enrico Fermi'. Course IL, Foundations of Quantum Mechanics, pp. 171-181. 1971.

[20] C.H. Bennett and G. Brassard. "Quantum Cryptography: Public key distribution and coin tossing". International Conference on Computers, Systems & Signal Processing. Bangalore, India. December, 1984.

[21] M.A. Pinto Bernabé. "Simulación de un protocolo de comunicación cuántica entre procesos en un ambiente distribuido". Tesis para optar al grado de Magíster en Ingeniería de Software. AICI, EUIIIS. Universidad de Tarapacá. Arica, Chile. 2009.

[22] L. Cáceres Alvares, M. Pinto Bernabé y P. Collao Caiconte. "Implementación de un Simulador de Criptografía Cuántica-Protocolo BB84". Jornadas Chilenas de la Computación. Temuco, Chile. Noviembre 2013.

[23] C.H. Bennett. "Quantum cryptography using any two non-orthogonal states". Physical Review Letters. Vol. 68 Nº 21, pp. 3121-3124. May, 1992. DOI: 10.1103/PhysRevLett.68.3121.

[24] R.L. Rivest, A. Shamir and L. M. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Commun. ACM. Vol. 21 Nº 2, pp. 120-126. February, 1978. ISSN: 0001-0782.

[25] Sun Microsystems and Oracle Corporation. "NetBeans Community". Netbeans. Fecha de consulta: Enero 2014. URL: https://netbeans.org/about/index.html

[26] J.M. Gálvez. "Manual para la observación de sondeos de globo piloto con un teodolito". South American Low Level Jet EXperiment. Septiembre 2002. Fecha de consulta: Junio 2013. URL: http://www.nssl.noaa.gov/projects/pacs/salljex/archive/manuals/manual-teodolitos-v1.2.html

[27] National Institute of Standards and Technology. "Data Encryption Standard". Fecha de consulta: Enero 2014. URL: http://nvlpubs.nist.gov/nistpubs/sp958-lide/250-253.pdf

[28] J.M. Miret Biosca. "Criptografía con Curvas Elípticas". Universidad de Lleida. España. 2005. Fecha de consulta: Enero 2014. URL: http://www.criptored.upm.es/ guiateoria/gt_m044a.htm

[29] Institute for Quantum Computing. "Quantum computing 101". University of Waterloo. Waterloo, Canada. Fecha de consulta: Febrero 2014. URL: https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101

[30] G. Coulouris, J. Dollimore, T. Kindberg and G. Blair. "Distributed Systems: Concepts and Design". Addison-Wesley. 5*th edition*. Boston, Estados Unidos. 2011. ISBN: 978-0-13-214301-1.