Implementación de un Simulador de Criptografía Cuántica – Protocolo BB84

Luis Cáceres Álvarez, Miguel Pinto Bernabé y Patricio Collao Caiconte

Área de Ingeniería en Computación e Informática, EUIIIS
Universidad de Tarapacá
Arica, Chile

{lcaceres & mapintob}@uta.cl

patricio.collao@alumnos.uta.cl

***Resumen* - El propósito del presente trabajo de investigación, consistió en la realización de una aplicación de criptografía cuántica que lograra simular el protocolo BB84. El estudio de los diversos protocolos de comunicación cuántica permite seleccionar el protocolo a simular en la aplicación, en este caso el protocolo BB84. Con toda esta información se pasó a la definición de los requerimientos de la aplicación, necesarios para establecer los límites de la aplicación. La definición de requerimientos da paso a la definición de la arquitectura de software y la plataforma de programación a utilizar en la etapa de desarrollo. La implementación de la aplicación permite aunar todo el trabajo de análisis y diseño realizado, logrando los resultados esperados. La etapa de pruebas permite testear la aplicación con respecto a diferentes largos de claves comunes a todas las aplicaciones de criptografía. Por tanto, se propone una alternativa más de seguridad a las aplicaciones que basan su seguridad en algoritmos tradicionales de criptografía, enfocándonos especialmente en la distribución segura de una clave. Por ello, es que en los resultados de las pruebas se analiza la fortaleza de la clave compartida por el protocolo, a través de pruebas sobre los largos de las claves, que permitieron concluir que el protocolo tiene un mejor comportamiento con una clave de largo inicial de 128 bits de entrada.**

Palabras Clave* - *Criptografía Cuántica, Protocolo Cuántico BB84, Simulador BB84.

I. INTRODUCCIÓN

El mundo de la industria y sobre todo el de las comunicaciones está cambiando rápidamente. La mayor fuente de poder es la información, con lo cual el mundo de las comunicaciones adquiere todavía mayor relevancia. Con este planteamiento social, no es de extrañar que la gente se preocupe cada vez más por la seguridad de sus comunicaciones [1].

Por otra parte, otro factor de gran importancia en nuestra sociedad es el tiempo. Vivimos en una sociedad, donde por ejemplo, una transacción comercial hecha en unos segundos antes o después puede suponer la pérdida o ganancia de cuantiosas sumas de dinero. En este contexto, en la actualidad se realizan muchas transacciones vía Internet, como la compra y venta de bienes y servicios, la utilización de tarjetas de crédito y cuentas bancarias para el pago de cuentas y transferencia de fondos. En dichas transacciones es necesario lograr establecer una comunicación segura entre los entes participantes, así como también es necesario proteger la información que se intercambia en una transacción. Para lograr estos objetivos existen diversas implementaciones de criptografía como las Firmas Electrónicas o Digitales [2], Protocolos de Seguridad como SSL [3], Certificados Digitales [4], Public Key Infrastructure [5], entre otras alternativas que se utilizan para proteger los datos y establecer una comunicación segura.

De estas alternativas de protección de la información, las Firmas Digitales tienen el objetivo de reemplazar la firma autógrafa tradicional por una firma electrónica que nos permita firmar documentos digitales con la misma validez que una firma convencional. La Firma Digital está compuesta de dos procedimientos: firma y verificación, los cuales se implementan mediante criptografía asimétrica [6]. Sin embargo, el esquema de Firma Digital basa su seguridad en una clave privada y en la imposibilidad matemática de factorizar números enteros grandes. Pues bien dicha seguridad puede ser quebrantada o mejorada con la llegada de la computación y criptografía cuántica.

Hellman y Scolnik [7] sostienen que la criptografía cuántica está aún en un estado embrionario y hasta dentro de 30 años no se verán sus primeras aplicaciones prácticas, que romperán con facilidad los actuales sistemas de cifrado. Mientras tanto, ha empezado una carrera paralela para proteger la información que debería seguir siendo secreta cuando irrumpa la criptografía cuántica. A partir de esta información es que surge la idea de este trabajo de investigación de contribuir con el esquema actual de seguridad de las firmas digitales, el cual se basa en algoritmos de criptografía simétrica y asimétrica, con una simulación de un protocolo cuántico. Dicho protocolo permitirá compartir una clave, que puede ser usada en el algoritmo de criptografía simétrica de la firma digital, lo cual mejoraría en cierta medida la seguridad de las firmas digitales.

Para una mejor comprensión, este artículo ha sido estructurado en 6 secciones, comenzando con la Introducción, para luego seguir con la Relevancia de la Criptografía Cuántica, Protocolo de Comunicación Cuántica, Simulación del Protocolo de Comunicación Cuántica, Modelo de la arquitectura cuántica en la aplicación BB84, Análisis y Pruebas de la Aplicación y por último la sección de Conclusiones.

II. Relevancia de la Criptografía Cuántica

El objetivo de la criptografía es asegurar que un mensaje secreto sea transmitido entre dos usuarios de modo que cualquier "escucha" no pueda leerlos. En la criptografía clásica, en general se acepta que el algoritmo one time pad o cuaderno de un solo uso, es uno de los sistemas de cifrado más seguros. Sin embargo, es difícil para todos los sistemas clásicos de criptografía establecer una clave incondicionalmente segura entre los usuarios [8]. Afortunadamente aparece la criptografía cuántica para ayudarnos en esta distribución de claves. Este enfoque utiliza los principios de la mecánica cuántica para distribuir una clave secreta. Con el rápido desarrollo de la computación cuántica, los físicos teóricos han desarrollado un gran interés en las organizaciones de informática. Muchas populares y no tan populares técnicas de introducción a la computación cuántica y a sus campos han sido publicadas. Es por esto que se han desarrollado diferentes sistemas de computación cuántica, en busca de lograr dominar esta materia que nos permitirá dar el siguiente paso en el mundo de la computación. Sin embargo, no solo sistemas de computación cuántica se han desarrollado, paralelamente se han creado sistemas de criptografía cuántica. Desde la introducción del protocolo BB84 [9] y su primera aplicación práctica en 1992 [10], en la cual se logró transmitir información en una distancia de 30 cm, usando como medio de transmisión el libre espacio, grandes esfuerzos se han dedicado a ampliar la distancia de transmisión en la QKD[1].

La mayoría actual de las tecnologías criptográficas, como RSA[2], DES[3], ECC[4] y otros algoritmos, están basados en factorización, logaritmos discretos y operaciones exponenciales. El algoritmo de Shor [11] para un ordenador cuántico puede resolver de manera eficiente los problemas de ecuaciones exponenciales. De este modo, los sistemas de criptografía actuales podrían convertirse en inútiles y carentes de seguridad [12], claro cuando las computadoras cuánticas se conviertan en una realidad. Actualmente se encuentra en la Compañía de Computación Cuántica [13] uno de los primeros computadores cuánticos comerciales que prometen revolucionar la industria del cómputo, debido principalmente por su gran poder de cálculo. Así como también la Internet cuántica, que a nivel de laboratorios han demostrado ser una sólida prueba de comunicación segura [14]. La gran desventaja de estos proyectos de investigación, son sus altos costos y razón principal de utilizar otras herramientas que demuestren la rigurosidad de la criptografía cuántica a través de simuladores, que es el objetivo de este proyecto de investigación.

A. *Simulaciones de Criptografía Cuántica*

Una alternativa a los sistemas de comunicación son los modelos de simulación cuántica de Zhang, et al [15], que nos dan una noción de estas simulaciones con la siguiente clasificación:

- Lenguajes de Programación: este tipo de simulación desarrolla un lenguaje de programación que simula la computación cuántica. Se implementan operaciones cuánticas básicas y se especifica una serie de reglas gramaticales basadas en la plataforma, que es adoptada para aplicar estas operaciones. Un ejemplo muy usado es QCL (Quantum Computation Language) que es uno de los programas aprobados popularmente [16]. Tiene su propio programa de construcción y da apoyo a variables, bucles, subrutinas y saltos condicionales.
- Paquete de computación Cuántica: este tipo de simulación se desarrolla sobre un paquete de software que sirve para utilizarse como una API.

Podemos agregar a esta clasificación, la propuesta de Zhang, et al [15], la cual podemos apreciar en la Fig. 1.

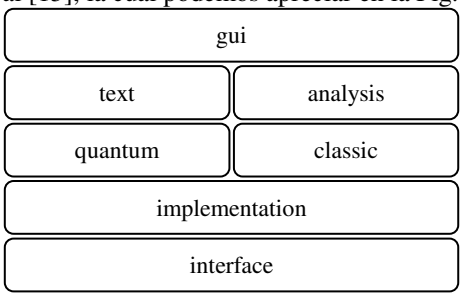

Fig. 1 Propuesta de Capas (Zhang, et al [15]).

Zhang, et al, después de analizar las simulaciones de computación cuántica y de compararlas con otros métodos de simulación, definieron el modelo de la Figura 1. En él proponen una arquitectura compuestas por 5 capas y 7 módulos, esto con el propósito de garantizar flexibilidad, fiabilidad, mantenibilidad y extensibilidad del modelo de simulación criptográfica cuántica que proponen.

III. Protocolo de Comunicación Cuántica

Uno de los problemas de mayor dificultad práctica a la hora de llevar a cabo una comunicación segura mediante un sistema de clave privada es la distribución segura de las claves. Las leyes de la mecánica cuántica permiten abordar el problema de la distribución segura de claves privadas. Los comunicantes pueden transmitir la clave privada a través de un canal cuántico. Por ejemplo, un cable de fibra óptica. En este

[1] QKD: Quantum Key Distribution (Distribución de claves cuánticas)

[2] Algoritmo asimétrico cifrador de bloques, fue descrito en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT; las letras RSA son las iniciales de sus apellidos.

[3] Data Encryption Standard (DES) es un algoritmo cifrador de bloques.

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

caso, los estados de polarización de un fotón se pueden usar para diseñar un protocolo criptográfico cuántico para la distribución de una clave aleatoria de un solo uso.

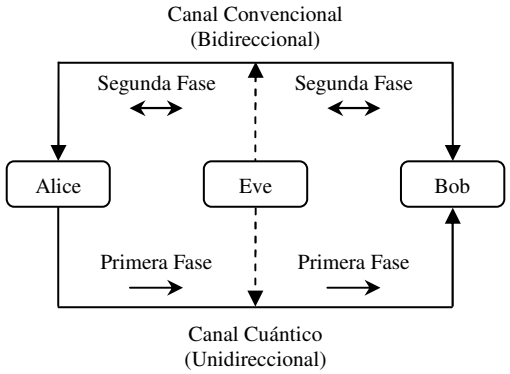

Fig. 2 Modelo de Comunicación Cuántica.

Como se muestra en la Fig. 2, en estos protocolos de criptografía cuántica existen dos canales, uno cuántico por el cual se transmite la clave (Primera Fase) y otro convencional por el cual se comunican los participantes en la comunicación (Segunda Fase). A continuación abordamos el protocolo de comunicación cuántica BB84, para su análisis y posterior implementación a través de una simulación.

A. Protocolo BB84

Este protocolo fue propuesto por Charles Bennet y Gilles Brassard en 1984 [9]. La idea es transmitir una clave binaria por un canal inseguro. Para transmitir el bit 0, Alice (el emisor) puede elegir al azar la base $\{|0\rangle,|1\rangle\}$ (a la que llamaremos esquema +) y considerar $0\cong|0\rangle$ y $1\cong|1\rangle$, o la base $\{|–\rangle,|+\rangle\}$ (a la que llamaremos esquema ×) y considerar $0\cong|–\rangle$ y $1\cong|+\rangle$. Bob realizará una medición sobre el estado recibido eligiendo al azar entre el esquema + y el esquema × [17].

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves según nos indican en [17]:

1) Alice comienza a transmitir una secuencia aleatoria de 0 y 1, alternando los esquemas + y × en forma aleatoria.
2) Bob recibe la secuencia y va alternando las mediciones entre los esquemas + y × al azar.
3) Alice le transmite a Bob la sucesión de esquemas empleados.
4) Bob le informa a Alice en qué casos adivinó el esquema de origen.
5) Usando solamente los bits de los esquemas idénticos a dos puntas, ambos han definido una sucesión aleatoria de bits que servirá como *one-time pad* de encriptación para transmisiones futuras por cualquier canal.
6) Alice y Bob intercambian hashes de las claves para aceptarla o descartarla.

En la Fig. 3, se muestra un ejemplo gráfico del intercambio de claves y de coincidencias para el establecimiento de la comunicación entre Alice y Bob.

Esquemas de Alice	×	+	+	×	×	+
Valores de Alice	$\|–\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|–\rangle$	$\|0\rangle$
Esquemas de Bob	+	×	+	×	+	+
Valores de Bob	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$
Coincidencias			✓	✓		✓
Clave			0	1		0

Fig. 3 Ejemplo de Comunicación (Díaz y Samborski [17]).

Según [17] este protocolo es absolutamente inviolable. Supongamos que Eve espía el canal de comunicación entre Alice y Bob e intenta recuperar la clave. Eve está en la misma situación que Bob y no conoce cuál esquema es el correcto, + o ×. Por lo tanto elige al azar y se equivocará en promedio, la mitad de las veces (tal como si quisiera adivinar la clave directamente). En el paso 5 Alice y Bob se ponen de acuerdo en cuáles valores tomar en cuenta (las coincidencias de la secuencia de esquemas). Esta información no le sirve de nada a Eve porque sólo en la mitad de las veces habrá acertado, de manera que malinterpretará sus valores finales.

Además el QKD brinda un método para que Alice y Bob puedan detectar el potencial espionaje de Eve: Imaginemos que Alice envía un 0 con el esquema × (representado por $|–\rangle$), Eve usa el esquema + forzando al qubit a definirse como $|0\rangle$, ó $|1\rangle$. Si Bob usa el esquema × y mide $|–\rangle$ coincide con lo enviado por Alice, pero si mide $|+\rangle$, Alice y Bob descubrirían esa discrepancia durante el intercambio de hashes, por lo tanto descartarían el bloque.

IV. Simulación del Protocolo de Comunicación Cuántica

Se justifica la implementación del protocolo BB84, principalmente por ser el primero que tiene un valor histórico en el mundo de la criptografía cuántica. Además es tomado como referencia en varios artículos de criptografía, por ser la primera aproximación de un protocolo cuántico y una base para crear nuevos protocolos cuánticos o variantes que surgen a partir de él, como lo es el protocolo B92 [18][19].

A. Requerimientos de la Aplicación BB84

Los requerimientos son una descripción de las necesidades de la aplicación. La meta principal en esta etapa es identificar lo que en realidad se necesita.

Requerimientos Funcionales: Las funciones del sistema son lo que éste deberá hacer y las identificamos a continuación:

- Generar la secuencia de números binarios que será transmitida.
- Generar el esquema que se utilizará en el cifrado de la secuencia.
- Permitir transmitir la secuencia cifrada por algún canal de comunicación.
- Permitir medir la secuencia cifrada.
- Permitir transmitir el esquema por algún canal de comunicación.
- Permitir comparar los esquemas utilizados en el cifrado de la secuencia.

- Permitir intercambiar los resúmenes de las claves en común.
- El sistema deberá poder funcionar de forma distribuida.

Requerimientos no Funcionales: No es suficiente con identificar los requerimientos funcionales, existen otras influencias que pueden condicionar el éxito de la aplicación, es por esto que también se consideran los siguientes requerimientos:

- El sistema será tolerante a fallas.
- El sistema presentará una interfaz amigable.
- El sistema deberá ser fácil de usar.
- El sistema realizará un uso eficiente de la memoria.

V. Modelo de la Arquitectura Cuántica usada en la Aplicación BB84

La arquitectura que tendrá la aplicación, será la de un modelo cliente/servidor usando la tecnología de Java RMI para la comunicación distribuida. Por tanto, esta es una razón elegir a Java como la plataforma y lenguaje de programación a utilizar en la aplicación.

A. Diseño de la Aplicación

Con los requerimientos funcionales y no funcionales definidos en las secciones anteriores, además de la arquitectura y lenguaje de programación a utilizar, ya sólo queda definir el modelo la aplicación a implementar.

B. Definiciones Previas

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

- **Secuencia**: Conjunto de números binarios que se transmiten en el canal de comunicación. 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. Ejemplo de esquemas: Sean las bases A=⊕ y B=⊗. Entonces un esquema válido sería el siguiente:

  ⊕⊗⊗⊕⊕⊕⊗⊗…⊕.

- **Secuencia cifrada:** conjunto de símbolos que representan el cifrado de la secuencia en las bases elegidas. Ejemplo de valores cifrados: Sean las bases A=⊕y B=⊗, donde tenemos que en la base ⊕ el bit 0 se representa por $|0\rangle$ y el bit 1 se representa por $|1\rangle$, mientras que en la base ⊗, el bit 0 se representa por $|-\rangle$ y el bit 1 se representa por $|+\rangle$. De esta forma la secuencia "01010100" si es cifrada con el esquema "⊕⊗⊗⊕⊕⊕⊗⊗" sería la siguiente:

  $|0\rangle|+\rangle|-\rangle|1\rangle|0\rangle|1\rangle|-\rangle|-\rangle$.

C. Implementación de la Aplicación

En esta sección se muestra la implementación de la aplicación del simulador criptográfico cuántico, que en su etapa inicial de pruebas se desarrolló en modo consola, una vez funcionando correctamente esta aplicación se extendió su comportamiento local a uno distribuido con su respectiva interfaz de usuario.

D. Configuración del Receptor/Emisor en el Ambiente Simulador

En la Fig. 4 (a – d), se muestran los pasos realizados en la configuración del receptor (máquina 1).

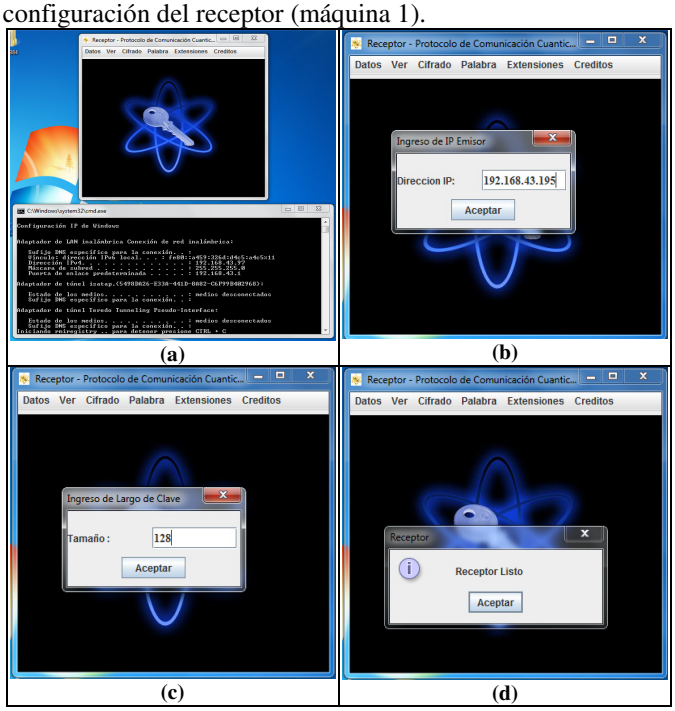

Fig. 4 Configuración del receptor en el simulador cuántico BB84.

a. El Receptor abre su sesión. En la parte inferior se inició rmiregistry por consola, mostrando también la IP del mismo.
b. En el Receptor se ingresa la dirección IP del Emisor.
c. En el Receptor se ingresa el tamaño inicial de la clave a establecer.
d. El Receptor informa que está listo para comenzar el establecimiento de la clave.

Del mismo modo, la configuración del emisor (máquina 2) procede similarmente, como muestra a continuación:

a. El Emisor abre su sesión. En la parte inferior se inició rmiregistry por consola, mostrando también la IP del mismo.
b. En el Emisor se ingresa la dirección IP del receptor.
c. En el Emisor se ingresa el tamaño inicial de la clave a establecer.

En el Emisor se selecciona "Iniciar" el establecimiento de la clave, seleccionando la opción en el menú Cifrado.

E. Proceso de Comunicación Segura del Simulador

En esta etapa se establece la comunicación segura entre el emisor y receptor, una vez realizada la configuración de ambos (como se mostró en la sección anterior) y que permite a continuación informar que se ha iniciado el proceso de distribución de la clave entre el emisor y el receptor. Luego, se da inicio al cifrado del mensaje a enviar entre ambas entidades participantes. La Figura 5 (a – h), muestra los pasos que se deben ejecutar para establecer la comunicación segura entre el emisor y el receptor.

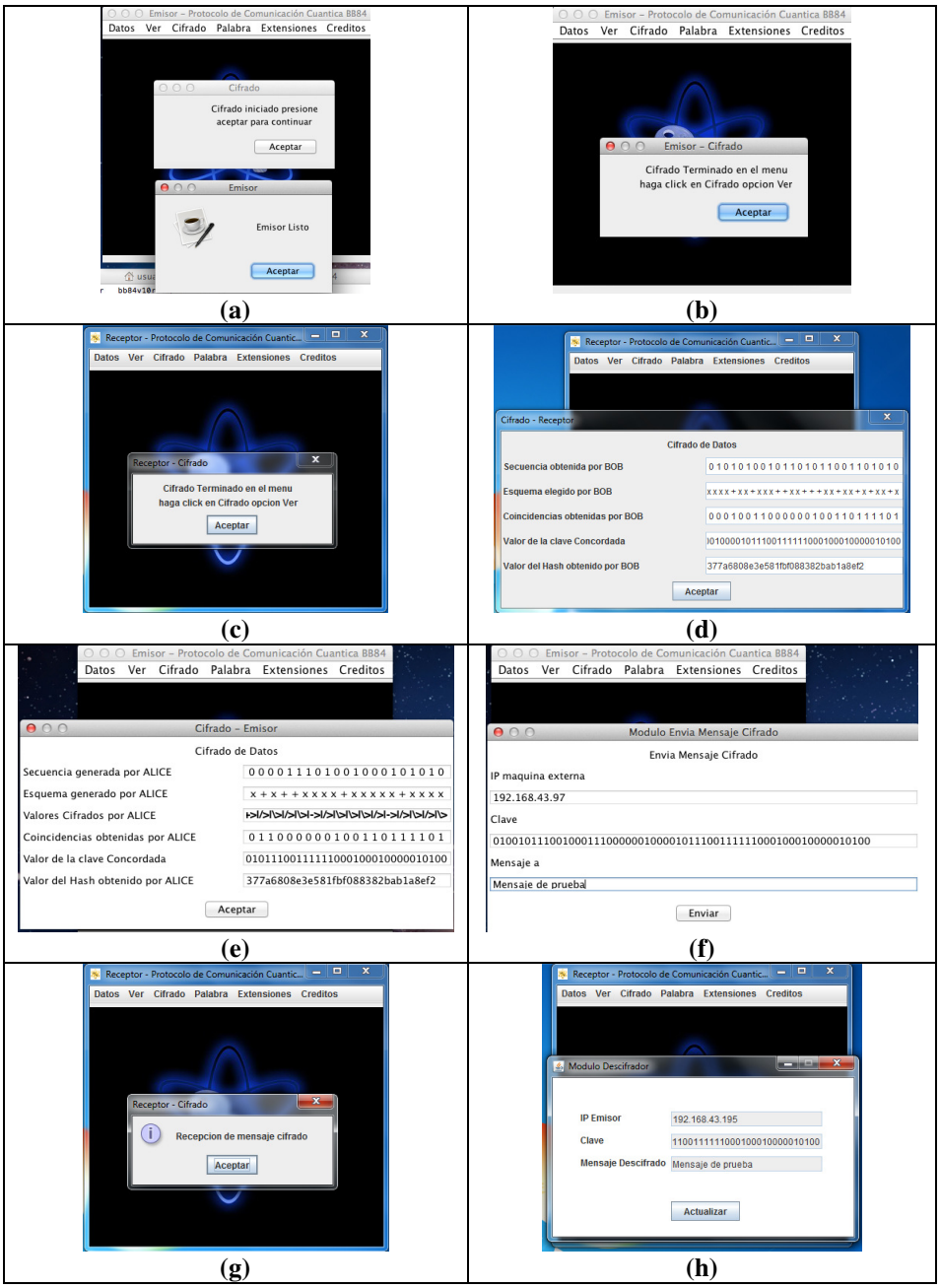

Fig. 5 Establecimiento de la comunicación segura entre el emisor y el receptor, una vez distribuida la clave que permite cifrar el mensaje.

a. El Emisor informa que ha iniciado el proceso de distribución de clave, dando aviso que está listo.
b. El Emisor informa que ha terminado. Por lo que ya se ha establecido una clave entre Emisor y Receptor.
c. El Receptor informa que ha terminado. Por lo que ya se ha establecido una clave entre Emisor y Receptor.
d. En el Receptor, tras seleccionar "Ver" en el menú de "Cifrado", muestra la información del proceso recién terminado, desde la perspectiva del mismo.
e. En el Emisor, tras seleccionar "Ver" en el menú de "Cifrado", se muestra la información del proceso recién terminado, desde la perspectiva del mismo.
f. El Emisor envía un mensaje cifrado con el algoritmo AES, y la clave simétrica que acordó con el Receptor.
g. El Receptor informa que ha recibido un mensaje cifrado.
h. El Receptor rescata el mensaje cifrado, utilizando el algoritmo AES, y la clave simétrica que acordó con el Emisor.

VI. Análisis y Prueba de la Aplicación

En esta sección se describirán las pruebas correspondientes a la aplicación. En primer lugar, se definirán los requerimientos necesarios para ejecutar la aplicación. En seguida, procederemos a testear la aplicación con diferentes valores de entradas, que corresponden a los largos de las claves, lo cual nos permitirá obtener largos finales que nos servirán como medida de la fortaleza de la clave.

A. *Pruebas de la Aplicación*

Para realizar estas pruebas se utilizaron distintas clases de computadores, con sus respectivos sistemas operativos instalados (Windows o Linux) y los cuales se encuentran en

diferentes redes. Para estas pruebas se utilizó la Tabla I, en la cual se tienen los largos comunes para las claves que se usan en criptografía simétrica.

TABLA I
LARGO DE CLAVES

Largo de claves		
8 bits	64 bits	512 bits
16 bits	128 bits	1024 bits
32 bits	256 bits	2048 bits

Caso I: en esta prueba ambos computadores comparten características similares y el mismo sistema operativo instalado, además se encuentran en la misma red privada. Esto debido a que se encuentran conectados mediante un router local, al cual acceden mediante la puerta de enlace 192.168.0.1. Con estos datos de entrada: las direcciones IP tanto del Emisor como el receptor y los largo de las clave se obtuvieron los resultados de la Tabla II.

TABLA II
RESULTADO DE LA PRUEBA 1 DE LA APLICACIÓN.

Largo Inicial	Largo Final	Cant. Bits perdidos	Tiempo (seg.)
8	3	5	2
16	11	5	2.8
32	16	12	9.7
64	33	31	22.5
128	74	56	43.6
256	119	137	80
512	264	248	167.3
1024	487	537	316.3
2048	1014	1034	628.6

De acuerdo a esta tabla de resultados, obtenemos el gráfico la Fig. 6, en el cual podemos observar que alrededor del 50% en promedio de los bits del largo inicial son usados como clave final. Estos resultados se deben a que los bits que son generados aleatoriamente en el protocolo cuántico antes de ser enviados por el canal de comunicación, son cifrados aleatoriamente por una de las dos bases cuánticas generadas.

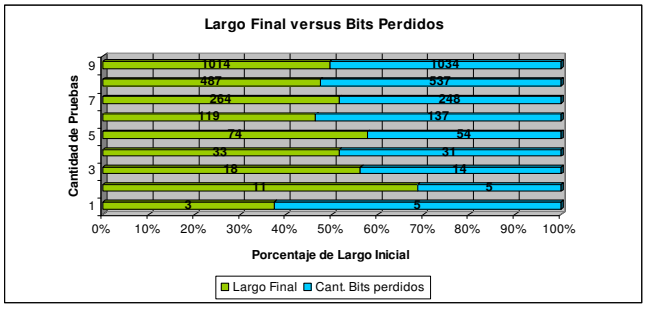

Fig. 6 Gráfico del Largo Final y Cantidad de bits perdidos.

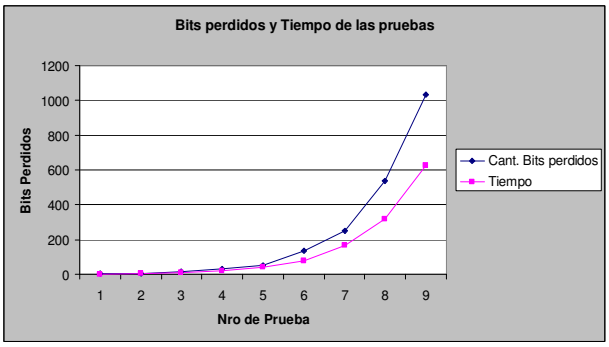

Fig. 7 Gráfico de Bits perdidos versus Tiempo de las pruebas.

En el gráfico de la Fig. 7, podemos observar que a medida que aumenta la cantidad de bits perdidos, también aumenta la cantidad de tiempo empleada en la prueba, esto se debe a que se tiene un largo inicial de clave más largo con cada prueba.

Caso II: en esta prueba ambos computadores compartes características similares, sin embargo, poseen distinto sistema operativo instalado, además se encuentran en distintas redes. El primer computador está en la subred 192.168.27.0, mientras que el segundo computador se encuentra en la subred 192.168.28.0. Estos computadores se encuentran conectados mediante dos routers, uno con la puerta de enlace 192.168.27.1 y el otro con la 192.168.28.1. Para esta prueba como para la anterior se utilizó la tabla 1, en la cual se definieron los largos comunes que se usan como claves. Con estos datos de entrada más las direcciones IP, se obtuvieron los resultados de la Tabla III.

TABLA III
RESULTADO DE LA PRUEBA 2 DE LA APLICACIÓN.

Largo Inicial	Largo Final	Cant. Bits perdidos	Tiempo (seg)
8	5	3	2,2
16	11	5	6,1
32	14	18	11,8
64	33	31	28
128	66	62	49,1
256	131	125	92,3
512	257	255	175
1024	497	527	327,9
2048	1043	1005	637.7

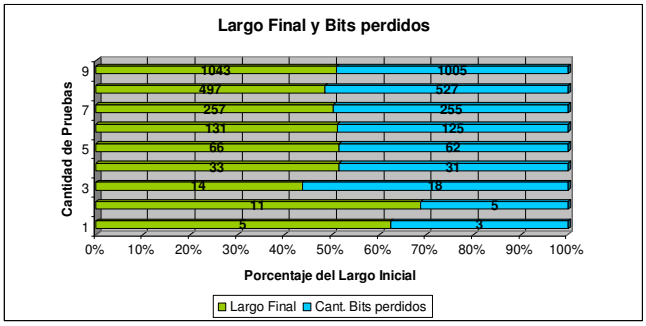

Fig. 8 Gráfico del Largo Final y Cantidad de bits perdidos.

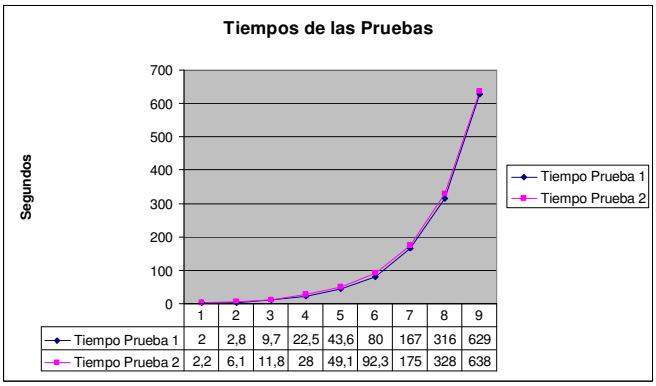

Fig. 9 Gráfico de Tiempos de las pruebas.

Con estos datos podemos obtener el gráfico de la Fig. 8, en el cual podemos observar que al igual que el caso I, se sigue manteniendo el resultado en el cual alrededor del 50% de los bits del largo inicial son usados como clave final.

El gráfico de la Fig. 9 nos muestra los tiempos de las pruebas realizadas, donde podemos observar que la prueba 2 toma más tiempo que la prueba 1, producto de que se encuentran en redes distintas tanto el emisor como el receptor. El grado de aumento de tiempo es de unos 8 segundos en promedio.

VII. Conclusiones

Para el desarrollo del trabajo de investigación se seleccionó el protocolo BB84, por ser el primer protocolo cuántico creado y porque ha sido la base para crear otros protocolos como el B92. En este contexto las pruebas de la aplicación, en un primer caso representado en un ambiente de red privado y otra de redes distintas, 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 en ambos casos de prueba demuestran que usando este protocolo se pierden alrededor de un 50% 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. Se concluye por tanto de los resultados obtenidos, que se comporta mejor con una clave de 128 bits de largo inicial, para lograr como largo final de clave una de 64 bits aproximadamente y que la única diferencia sustantiva está en función de los tiempos de prueba, producto principalmente a que en el caso de redes distintas se alcanza a un tiempo aproximado de 8 segundos promedio de aumento que el caso de una red privada. Por último, para consolidar los resultados y dando continuidad a la línea de investigación, es que actualmente se están realizando pruebas con el simulador del protocolo cuántico E91. De esta manera, se podrá realizar un análisis comparativo, con el propósito de probar las fortalezas de ambos protocolos.

References

[1] Ortega, S.: “Aplicaciones de las Curvas Elípticas en Criptografía”, Tesis Doctoral, Universidad de Valladolid (España) en 1996, pp. 3.

[2] Reyes, A. “La Firma Electrónica y la Entidades de Certificación”, Tesis de Doctorado, Octubre 2002, pp. 164-240.

[3] David, W., Schneier, B. “Analysis of the SSL 3.0 Protocol”, The second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 1996, pp 29-40.

[4] Ministerio Secretaría General de la Presidencia “Manual Operativo: Documentos Electrónicos y Firma Electrónica en los Servicios Públicos y la Administración del Estado”, Septiembre 2003, página 15-16.

[5] Kuhn, R., Hu, V., Polo, T., Chang, S., “Introduction to Public Key Technology and the Federal PKI Infrastructure”, February 2001, pp 15-27.

[6] Diffie, W., Hellman, M.E. “New Directions in Cryptography”, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp 644-654.

[7] Hellman, M., Scolnik, H. “El Desarrollo de la Criptografía Cuántica Descifrará Todas las Claves Actuales”. Día Internacional de la Seguridad en la Universidad Politécnica de Madrid. Notas de Prensa y Noticias relacionadas con la Cátedra, Enero 2008.

[8] Gao, F., Qin, S., Wen, Q., Zhu, F. : “One-time Pads Cannot be Used to Improve the Efficiency of Quantum Communication”, Physics Letters A, Volume 365, Issues 5-6, 11 June 2007, Pages 386-388..

[9] Bennet, C., Brassard, G.: “Quantum Cryptography: Public Key Distribution and Coin Tossing”. Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing, year 1984, pp.175-179.

[10] Bennet, C., Brassard, G., Bessette, F., Smolin, J.: “Experimental Quantum Cryptography”, Journal Cryptology 1992, Volume 5, Issue 1.

[11] Shor, P.: “Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. SIAM J.Comp., 26 (5), pp. 1484-1509, 1994.

[12] Chung, Y., Zhen, Y., Shyong, T.: “Unconditionally Secure Cryptosystems Based on Quantum Cryptography”, Information Sciences: an International Journal, Volume 178, Issue 8 April 2008 table of contents Pages 2044-2058.

[13] Anthony, S.: “Quantum Computer Finally Proves its Faster than a Conventional PC, but Only Just”. Ver página Web: http://www.extremetech.com/. Mayo 2013.

[14] Hughes, R, Nordholt, J, et. al.: “Network-Centric Quantum Communications with Application to”. Ver página Web: http://arxiv.org. Mayo 2013.

[15] Zhang, X., Wen, Q., Zhu, F.: “Object-Oriented Quantum Cryptography Simulation Model”, IEEE Computer Society, Third International Conference on Natural Computation (ICNC 2007).

[16] Ömer, B.: “QCL - A Programming Language for Quantum Computers”, la especificación se encuentra en la siguiente dirección web: http://tph.tuwien.ac.at/~oemer/qcl.html.

[17] Díaz, A., Samborski, J.: “Brevísima Introducción a la Computación Cuántica”, Departamento de Ciencias de la Computación, Universidad Nacional de Rosario. Ver página Web: http://www.fceia.unr.edu.ar/~diazcaro/. Abril de 2006.

[18] C.H. Bennett, “Quantum Cryptography Using any Two Nonorthogonal States”. Phys. Rev. Letter 68, pp.3121-3124, 1992.

[19] Montoya, F.: “Criptografía Cuántica, ¿Realidad o Ficción?”, Instituto de Física Aplicada, Departamento del Tratamiento de la Información y Codificación, Consejo Superior de Investigaciones Científicas. 2004.