Colegio Alemán Alexander von Humboldt

Computadoras Cuánticas ¿Revolución tecnológica o amenaza global?

Autores: Ruy Mariné Fernández del Valle, Miguel Ángel Gama Marroquín, Gregory Francis Maldonado Gordillo

Asesor: Profesor Nicolás Frank

Área de conocimiento: Ciencias Físico-matemáticas y de las Ingenierías

Disciplina: Computación y Tecnologías de la Información

Tipo de investigación: Documental

México D.F. 13 marzo de 2013

RESUMEN

El uso de computadoras cuánticas presenta obstáculos todavía insuperables para los avances de la tecnología actual, pero, de ser estos remontados, sería posible realizar cálculos computacionales imposibles para las computadoras digitales, todo esto en cuestión de segundos. La humanidad sería capaz de resolver problemas científicos y matemáticos muy complejos. Aunque todo esto tendría un gran significado para la ciencia, podría ser muy peligroso: Si el poder de una computadora cuántica fuera usado para mal, podría descifrar fácilmente los códigos de encriptación de contraseñas y datos personales enviados por internet, lo cual causaría grandes estragos económicos, sociales y políticos al poner la información en peligro.

Hacemos una investigación documental en la cual analizamos el funcionamiento de una computadora cuántica y los sistemas de encriptación actuales para encontrar una solución a este problema. Una computadora cuántica utiliza principios de la física cuántica para guardar información y hacer cálculos con ella. En lugar de utilizar bits binarios como una computadora digital, usa qubits cuánticos, que permiten guardar más de un valor a la vez y permiten procesar información paralelamente, incrementando la velocidad del cálculo. Aunque los sistemas de encriptación más comunes actualmente sirven perfectamente con computadoras digitales, podrían ser vencidos fácilmente por una computadora cuántica. Analizamos un sistema de encriptación cuántica y establecemos que las computadoras cuánticas no pueden interactuar con las digitales y no son una amenaza de seguridad.

Palabras clave: Computadoras, física, mecánica, cuántica, encriptación, algoritmo, amenaza

ABSTRACT

The use of quantum computers presents obstacles for current science that are yet to be overcome. Would this be achieved, it would be possible to make very complex computations in a matter of seconds, a feat unheard of in the realm of digital computers. With the help of quantum computers, humanity would have the ability to solve scientific and mathematical problems very easily. Although this would be very valuable in the field of science, it could also be very dangerous. If the technology of quantum computers fell into the wrong hands, it could be used i easily decipher the codes and methods of encryption used to transfer data online, which could cause significant sociopolitical problems by putting classified information in danger.

We use documentary research methods to analyze the functioning of a quantum computer and current systems of encryption in order to provide a solution to this problem. A quantum computer uses principles of quantum physics to store information and make computations. Instead of using binary bits, like a digital computer does, it uses quantum bits (*qubits*), that allow for the storage of more than one value at a time. This enables the computer to do parallel processing of information and increases it's calculation speed dramatically. Even though current systems of encryption serve their purpose when facing digital computers, a quantum computer could easily crack them.

We analyze a system of quantum encryption and establish that quantum computers cannot interact with digital computers, and are not a security threat.

Key words: Computers, quantum, physics, mechanics, encryption, algorithm, threat

INTRODUCCIÓN

PROBLEMA Y JUSTIFICACIÓN

El uso de computadoras cuánticas presenta obstáculos todavía insuperables para los avances de la tecnología actual, pero, de ser estos remontados, sería posible hacer cálculos computacionales imposibles para las computadoras digitales, todo esto en cuestión de segundos. La humanidad sería capaz de resolver problemas científicos y matemáticos, como hacer estudios bioquímicos, predicciones meteorológicas o búsquedas complejas en bases de datos, a una velocidad millones de veces mayor. Aunque todo esto tendría un gran significado para la ciencia y la calidad de vida de la sociedad moderna, tenemos la hipótesis de que también podría ser muy peligroso: Usando una computadora cuántica para mal, se podrían descifrar fácilmente los códigos de encriptación de contraseñas y datos personales enviados por internet, lo cual causaría grandes estragos económicos, sociales y políticos.

HIPÓTESIS

Las computadoras cuánticas usan partículas atómicas denominadas qbits para procesar información. A diferencia de un bit digital, un qubit cuántico puede guardar varios datos al mismo tiempo, lo cual se logra a través del uso de dos estados en un

átomo o la polarización de un fotón. A través de la superposición de estados cuánticos de una partícula, se puede representar un 1 o un 0 al mismo tiempo. Esto le permite a la computadora cuántica trabajar a velocidades increíbles.

OBJETIVO GENERAL

En esta investigación pretendemos analizar si la distribución de computadoras cuánticas para uso práctico presenta un peligro para la sociedad. Para esto, queremos estudiar más detalladamente el funcionamiento de las computadoras cuánticas, su forma de procesar información y cómo podrían interactuar con los sistemas de criptografía actual.

OBJETIVOS ESPECÍFICOS

1. Explicar cómo funciona una computadora cuántica y por qué es tan poderosa. 2. Identificar bajo qué condiciones se podrían producir computadoras cuánticas en el futuro y qué tan fácil de obtener serían éstas.
3. Analizar cómo funcionan los sistemas de codificación de información actualmente y que tan fácil sería modificar éstos para que no fueran fácilmente descifrables.

FUNDAMENTACIÓN TEÓRICA

Al ser el uso de computadoras cuánticas un tema polémico y rápidamente cambiante, no existe una sola teoría en la que nos hayamos basado para hacer nuestra investigación. Para tratar el funcionamiento de una computadora cuántica nos

basamos en el principio de la superposición cuántica, que dicta que un sistema cuántico tiene todo su posible estado al mismo tiempo, pero al ser medido u observado, sólo da un resultado. Para explicar un modelo posible de encriptación cuántica nos basamos en el protocolo *BB84*, diseñado por Charles H. Bennett y Gilles Bassard.

METODOLOGÍA DE INVESTIGACIÓN

Para poder alcanzar nuestro objetivo, hicimos una investigación documental que nos permite responder detalladamente las tres preguntas de las cuales consisten nuestros objetivos específicos. También nos pusimos en contacto con la compañía estadounidense D-Wave Systems, Inc., pionera de la computación cuántica, para entender cómo maneja su tecnología y cuál es su filosofía al distribuir computadoras cuánticas.

RESULTADOS

Antecedente: ¿Cómo funciona una computadora cuántica y por qué es tan poderosa?

Para entender el funcionamiento de una computadora cuántica es necesario analizar el de una computadora clásica. Una computadora trabaja con elementos llamados bits, que son bloques de información que pueden tener en un momento determinado uno de dos estados: negativo (0) o positivo (1). La computadora lee una secuencia de bits, y de acuerdo a la combinación de 0s y 1s que ésta contenga, puede descifrar un mensaje o una fracción de información codificada. En una computadora digital

solamente se puede realizar una lectura de información a la vez, ya que cada bit tiene sólo un estado. Aunque las computadoras modernas tienen procesadores muy potentes (una computadora comercial con un procesador de 2GHz puede leer 2,000,000,000 bits por segundo), éstas se ven limitadas naturalmente por su funcionamiento secuencial.

Se halla aquí la diferencia fundamental entre una computadora digital y una cuántica. Si se utilizan bases de la mecánica cuántica para guardar información se puede mejorar altamente el desempeño de las computadoras. La teoría de la superposición cuántica indica que una partícula subatómica puede tener varios ímpetus angulares intrínsecos (en inglés, *spins*) que son independientes el uno del otro.

En la física cuántica, el spin de una partícula determina en qué dirección (de dos direcciones posibles) se alinea cuando entra en un campo magnético. Si sobre una partícula reinan varios campos magnéticos, ésta puede alinearse también en otras direcciones. Por lo tanto una sola partícula puede tener más de dos estados cuánticos. Si se utilizan los spins de una partícula bajo distintos campos magnéticos para grabar información, se pueden guardar más de dos valores en una sola partícula (denominada *qubit* o *bit cuántico)*. Así se puede procesar más información en menos tiempo.

Hasta ahora han existido varias propuestas de cómo poner en práctica el concepto de la computación cuántica. A continuación presentaremos tres de las más importantes.

1. **Con resonancia magnética nuclear**: En 1998 Isaac Chuang del Laboratorio Nacional de Los Álamos, Neil Gershenfeld del MIT y Marc Kubinec de la Universidad de California (Berkley) crearon la primera computadora cuántica capaz de solucionar problemas sencillos. Ésta consistía de 2 qubits y, aunque su sistema se desintegraba en pocos nanosegundos, probó que las bases teóricas de la computación cuántica eran aplicables.

Los científicos disolvieron moléculas de cloroformo ($CHCl_3$) en agua a temperatura ambiente y usaron un campo magnético para orientar los spins de las partículas de carbón (primer qubit) e hidrógeno (segundo qubit). Posteriormente utilizaron el fenómeno de la resonancia magnética nuclear, dirigiendo ondas de radio de alta frecuencia hacia los núcleos atómicos, para cambiar el spin de éstos y crear superposiciones cuánticas. Con ayuda estos pulsos de radiación la computadora podía llevar a cabo algoritmos sencillos, aunque los cálculos que hacía no pasaban de ser triviales. En el año 2000, se creó una computadora de 7 qubits usando ese sistema.

2. **Con trampas electromagnéticas:** En el año 2000, científicos del NIST (National Institute for Standards and Technology) en Estados Unidos, bajo la coordinación del físico David Wineland, crearon una computadora de 4 qubits alineando cuatro iones de Berilio y enfriándolos con láser a poco arriba del cero absoluto (0 K o -273 ºC). Posteriormente sincronizaron los spins de las partículas

y usaron otro láser para introducir superposiciones. La capacidad de esta computadora tampoco logró rebasar la trivialidad.

3. **Con puntos cuánticos:** Otra posibilidad para lograr la computación cuántica es el uso de semiconductores, que son elementos cuyos electrones pueden cambiar de banda de acuerdo a su estado cuántico. Aplicando voltaje a los electrones, se puede controlar su paso por los denominados puntos cuánticos, pequeñas porciones de materia semiconductora que alojan a estos electrones libres, y medir su spin. Usando este método, se pueden crear chips que tienen varios puntos cuánticos iguales e incorporan un gran número de qubits. Se usa un campo magnético externo para controlar los spins, y un cableado de electrodos para hacer lecturas en los puntos cuánticos.

4. **Propuesta:** Aunque en la teoría se pueda hablar confiadamente del uso de la física cuántica para computar datos, en la práctica presenta varios problemas que aún no han podido ser resueltos. El más importante de éstos es el entrelazamiento cuántico. Para que un sistema computacional funcione, los qubits tienen que estar entrelazados, es decir, tienen que interactuar entre sí y depender de los demás qubits. Se siguen realizando investigaciones para lograr crear computadoras cuánticas estables, confiables y prácticas.

DISCUSIÓN

I: ¿Bajo qué condiciones se podrían producir computadoras cuánticas en el futuro y qué tan fácil de obtener serían éstas?

La ciencia de las computadoras cuánticas se encuentra todavía en desarrollo. Es difícil prever la presencia futura de computadoras cuánticas en el mercado y su disponibilidad al público. Por lo tanto no hemos podido responder esta pregunta concretamente.

Cabe mencionar que la primera computadora cuántica comercial fue producida en el año 2011 por la compañía estadounidense D-Wave Systems, Inc.

Nos pusimos en contacto con dicha compañía por correo electrónico buscando más información acerca de la computadora. Obtuvimos la siguiente respuesta:

“The system is comprised of a large shield room (3 meters X 3 meters X 2.5 meters) that houses a cryogenics system which in turn brings the processor down to operating temperature. We create an environment where the processor is shielded from external signals and magnetism. The operating temperature is close to absolute zero (0.020 Kelvin), where no energy exists, allowing superconductivity. In this extremely cold and quiet environment we are able to leverage quantum mechanics. The processor uses quantum annealing to determine optimality of a given set of inputs. It is not capable of running common software nor does it run any well-known operating system.

As you can imagine, the investment in research and development along with costs of building the systems is quite high. Accordingly, we have focused on marketing to

universities, government and *Fortune 500* companies whose budgets allow for expensive infrastructure of this kind."

Traducción: "El sistema consiste de una cámara protectora grande (3 metros X 3 metros X 2.5 metros) que aloja un sistema criogénico[1] que optimiza la temperatura del procesador para que éste pueda funcionar. Creamos un ambiente en el cual el procesador está aislado de señales externas y magnetismo. La temperatura de operación del procesador es cercana al cero absoluto (0.020 Kelvin), donde no existe energía y hay superconductividad. En este ambiente extremadamente frío y tranquilo, podemos aplicar la mecánica cuántica. El procesador usa recocido[2] cuántico para determinar la calidad óptima de cierto número de entradas. No es capaz de correr software convencional ni ningún sistema operativo conocido.
Como podrán imaginar, la inversión en investigación y desarrollo, junto con el costo de construir los sistemas, es muy alta. Por consiguiente, nos hemos concentrado en ofrecer este producto a universidades, instituciones gubernamentales y compañías del *Fortune 500* cuyo presupuesto alcanza para tener infraestructura de este tipo."

II. ¿Cómo funcionan los sistemas de codificación de información actualmente y que tan fácil sería modificar estos para que no fueran fácilmente descifrables?

Encriptación

[1]Criogenia: Estudia cómo alcanzar temperaturas muy bajas y el comportamiento de los elementos a esas temperaturas.
[2] Recocido: tratamiento térmico de un material para alterar su estructura

La encriptación es el proceso de transformar una información que se cree pertinente, en intangible. Esta información solo puede ser leída si es aplicada la clave correcta para descifrarla.

Se trata de un procedimiento para almacenar o transferir información que no pueda ser leída por terceros. Puede tratarse de contraseñas, números de tarjetas bancarias, conversaciones privadas o cualquier otro mensaje que se desee esconder.

La encriptación funciona a través de ciertos tratamientos a los códigos ASCII[3] de los mensajes, de modo que solo a través de la inversión del procedimiento se puede decodificar el mensaje.

Para volver indescifrable una cadena codificada, se intenta combinar la clave de encriptación con el mensaje, de manera que las probabilidades de descifrar la información sin conocer la clave sean muy bajas. El trabajo de desciframiento se hace tan prolongado que no existen esperanzas próximas, tanto para una persona, como para una computadora digital, de descifrar la información.

A continuación comentaremos los dos criptogramas básicos:

CIFRADO SIMÉTRICO

En la criptografía simétrica o *criptografía de clave secreta*, las partes implicadas en una comunicación acuerdan y comparten una clave secreta.

[3] ASCII: El código con el que una computadora procesa caracteres de texto convencionales. Se le asigna a cada símbolo un número en sistema binario.

Los datos se encriptan y se descifran usando la misma clave (motivo por el cual se denomina simétrica) y ésta solo debe ser conocida por los participantes para garantizar la seguridad del mensaje.

Este sistema es muy sofisticado y muy rápido. Actualmente existen diversos algoritmos muy potentes y robustos para hacer este tipo de cifrado. El grado de protección depende de la longitud de la clave secreta. Por estas razones es común cambiar la clave con frecuencia.

El mayor inconveniente de este sistema es la comunicación o distribución de la clave, que debe estar a cargo de medios seguros ya que si es interceptada, se puede ver comprometida la información.
Hoy en día, algunos de los algoritmos más usados son *DES, RC5* e *IDEA*

DES

El algoritmo de encriptación *DES (Data Encryption Standard)* fue desarrollado por la empresa IBM en 1976 y se basa en un sistema mono alfabético, con un algoritmo que consiste en la aplicación, varias permutaciones[4] y sustituciones. Al principio, el texto que será cifrado se somete a una variación del orden de sus elementos con bloques de entrada de 64 bits. Después, es sometido a dos funciones principales, primero la permutación de 8 bits y luego la sustitución con entrada de 15 bits.
El algoritmo cuenta con 16 etapas de cifrado y usa la clave simétrica de 64 bits (56 para la encriptación y 8 para la detección de errores).

[4] Permutación: Variación del orden o de la disposición de los elementos de un conjunto.

RC5

RC5 es el sucesor de *RC4; RC4* consistía en hacer un XOR[5] al mensaje con un arreglo aleatorio, que se desprende de la clave. *RC5* utiliza las rotaciones con dependencia de datos, en las cuales se incorporan rotaciones circulares de bits, que dependen de los datos introducidos.

RC5 permite tener diferentes longitudes de clave, aunque su exportación fuera de Estados Unidos con longitudes mayores a 56 bits está prohibida.

El sistema fue creado por la empresa RSA Data Security Inc., creadores del sistema *RSA*. Se trata de una de las empresas más importantes en el campo de la protección de datos.

IDEA

Creado en 1990 por Xuejia Lai y James Massey, trabaja con bloques de texto de 64 bits. Opera con 16 bits utilizando XOR y suma y multiplicación de enteros.

Es un sistema muy fácil de programar, debido a que el algoritmo de encriptación y desciframiento es muy parecido. Hasta ahora no ha sido roto, ya que supone una seguridad fuerte en contra de los ataques de fuerza bruta.

[5] XOR (Disyunción exclusiva): Operación lógica que evalúa el estado de dos operandos y da un resultado positivo si uno de estos operandos es falso y el otro verdadero.

IDEA utiliza textos en bloques de 64 bits y una clave de 128 bits, el proceso de encriptación consta de ocho pasos, todos idénticos excepto en los sub-bloques de la clave utilizados, terminando con una transformación de salida.

El algoritmo es de libre difusión y no está sometido a ninguna restricción.

CRIPTOGRAFÍA ASIMÉTRICA

La *criptografía asimétrica* o *criptografía de llave publica* se basa en el uso de dos claves diferentes, una para encriptar y la otra para descifrar.

Una de las claves es llamada clave privada y se usa solamente para encriptar los mensajes, mientras la otra, llamada clave pública, se usa para descifrar la información. Las dos claves tienen propiedades matemáticas especiales, de tal forma que se generan al mismo tiempo y están ligadas la una a la otra, pero su relación es lo suficiente compleja para que no se pueda obtener a partir de una la otra. Es por ello que a veces estas claves las crea un algoritmo y no el usuario (además, estas claves suelen ser de largas longitudes).

Los algoritmos asimétricos tienen su base en funciones matemáticas fáciles de resolver en un sentido pero muy difíciles de resolver es el sentido inverso, a menos que se tenga la clave privada.

La mayor ventaja de la criptografía asimétrica, frente a la simétrica, es que el algoritmo de cifrado puede ser de dominio público y que la clave privada no es puesta en peligro

ya que se encuentra en manos del propietario. Como desventaja, los algoritmos son mucho más lentos y dificultan la implementación del sistema.

Entre los algoritmos de clave pública más importantes están el *Diffie-Hellman* y *RSA.*

Diffie-Hellman

El algoritmo fue creado por Whitfield Diffie y Martin Hellman en 1976 y supuso una gran revolución para la criptografía. Fue punto de partida para los sistemas asimétricos.

Su importancia se debe a ser el inicio de éstos, ya que en la práctica es usado para el intercambio de claves simétricas, y es usado es varios sistemas seguros como *VPN (Virtual Private Network)* y *SSL (Secure Socket Layer)*.

Diffie-Hellman se basa en la potencia de números y en la función mod[6]. Uniendo el concepto matemático se obtiene la potencia discreta de un numero con x = y mod z. El cálculo es fácil, pero su función inversa, el logaritmo discreto, no tiene solución analítica para números grandes.

[6] Mod: Operación matemática que calcula el restante al ser divididos dos números enteros. Por ejemplo: 9 mod 2 = 1 ya que 9/2 = 4 con un restante de 1

RSA

El algoritmo *RSA* es el más popularmente conocido. Su creador fue la compañía RSA Data Security, Inc., en 1978.

RSA permite el uso de varias longitudes, aunque se aconseja que estas sean menores de 1024 bits (se ha logrado romper claves de hasta 512 bits, aunque esto tardó 5 meses y trabajaron 300 ordenadores).

RSA se basa en ser una función segura, ya que trabaja con exponenciación modular, que es fácil de hacer pero su operación inversa, la extracción de raíces de modulo x, no es factible al menos que conozca la factorización de e.

Si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Ahora que hemos hablado de los sistemas de seguridad más usados, explicaremos de qué forma se podría atacar un algoritmo *RSA* y si una computadora cuántica sería capaz de hacerlo.

Fuerza Bruta

En este caso se intenta aplicar todas las claves privadas posibles, una por una, lo cual lo vuelve muy lento y poco práctico.

Ataques matemáticos

Existen varios enfoques pero todos quieren obtener el mismo resultado, factorizar el producto de los dos números primos.

Diffie-Hellman se basa en la potencia de números y en la función mod[7]. Uniendo el concepto matemático se obtiene la potencia discreta de un numero con x = y mod z. El cálculo es fácil, pero su función inversa, el logaritmo discreto, no tiene solución analítica para números grandes.

RSA

El algoritmo *RSA* es el más popularmente conocido. Su creador fue la compañía RSA Data Security, Inc., en 1978.

RSA permite el uso de varias longitudes, aunque se aconseja que estas sean menores de 1024 bits (se ha logrado romper claves de hasta 512 bits, aunque esto tardó 5 meses y trabajaron 300 ordenadores).

RSA se basa en ser una función segura, ya que trabaja con exponenciación modular, que es fácil de hacer pero su operación inversa, la extracción de raíces de modulo x, no es factible al menos que conozca la factorización de e.

[7] Mod: Operación matemática que calcula el restante al ser divididos dos números enteros. Por ejemplo: 9 mod 2 = 1 ya que 9/2 = 4 con un restante de 1

Si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Ahora que hemos hablado de los sistemas de seguridad más usados, explicaremos de qué forma se podría atacar un algoritmo *RSA* y si una computadora cuántica sería capaz de hacerlo.

Fuerza Bruta

En este caso se intenta aplicar todas las claves privadas posibles, una por una, lo cual lo vuelve muy lento y poco práctico.

Ataques matemáticos

Existen varios enfoques pero todos quieren obtener el mismo resultado, factorizar el producto de los dos números primos.

El principio del protocolo *BB84* se puede utilizar para transmitir claves seguras.
La criptografía cuántica hace uso de dos canales, un canal público y un canal cuántico. El canal cuántico tiene un sentido único y generalmente es una fibra óptica (los qubits son en este caso, fotones), mientras que el canal público es de dos vías. El sistema se puede explicar a través del siguiente ejemplo:

Supongamos que una persona (Miguel) le quiere enviar una clave a otra (Ruy) a través del canal cuántico. El valor del qubit es codificado dentro de la propiedad de un fotón,

usando la polarización. La polarización es la dirección de oscilación de su campo eléctrico.

Para recibir la clave se utilizan diferentes filtros, ya sea para la polarización vertical (polarización 0), u horizontal (polarización 1).

Al enviar Miguel la clave, Ruy elige que filtro usar. Al pasar el fotón correcto por el filtro correcto su polarización no cambia. Si pasa por uno incorrecto su polarización cambia de forma aleatoria.

Los dos registran, ya sea las orientaciones enviadas o recibidas, y por el canal convencional Ruy le manda a Miguel la secuencia de filtros usados y Miguel le dice en cuáles casos usó el filtro correcto. Así, saben los dos en qué casos sus qubits deberían ser idénticos. Estos qubits formaran su clave.

Finalmente verifican el nivel de error de la clave, haciendo pública una parte de sus qubits.

Ahora si un tercero intenta espiar la comunicación no podrá medir los fotones correctamente al no saber que filtro usar y causará un error.

Si al verificar el nivel de error encuentran diferencias en sus qubits Miguel y Ruy, sabrán que los están espiando, provocando que elijan una nueva clave. Luego podrán mandar el mensaje a través de métodos convencionales.

CONCLUSIONES

Las computadoras cuánticas son sin duda alguna un avance tecnológico muy poderoso, que marca el siguiente paso en la computación modera. A pesar de estar todavía en desarrollo y aún no ser la tecnología indicada para el uso práctico de la computación, las computadoras cuánticas prometen mucho para el futuro.

En este trabajo teníamos como objetivo analizar si las computadoras cuánticas podían ser un peligro para la sociedad. Nuestra hipótesis era que sí, ya que usando su poder para mal se podrían romper rápidamente las claves de encriptación actuales y poner en peligro la información de millones de personas. Esto causaría estragos económicos, políticos y sociales muy graves.

Para probar nuestra hipótesis, nos pareció muy importante tomar en cuenta los resultados de nuestros objetivos II y III.

En la respuesta que obtuvimos de D-Wave, nos informaron que las computadoras cuánticas no son capaces de correr ni sistemas operativos, ni software conocidos. Esto quiere decir que una computadora cuántica sólo puede hacer cálculos independientes, pero no interactuar con el mundo de las computadoras digitales. Esto elimina todo peligro de que una computadora cuántica fuera usada para infiltrarse en sistemas creados para computadoras digitales y refuerza la posición de las computadoras cuánticas como un instrumento científico muy valioso.

Al investigar sobre los sistemas de encriptación, notamos que la encriptación cuántica tiene un funcionamiento completamente diferente a la digital.

Nos quedó claro que comparar computadoras cuánticas con computadoras digitales no es válido, ya que las dos tecnologías tienen estructuras internas completamente diferentes, que no pueden interactuar entre sí.

Por estas razones hemos establecido que nuestra hipótesis era falsa. Nos da gusto darnos cuenta de que las computadoras cuánticas son una revolución tecnológica y no una amenaza global, ya que en el futuro serán un instrumento fundamental de la investigación científica.

BIBLIOGRAFÍA

- Bader, Franz, *Physik Sek II*, Braunschweig, Schroedel, 2000.

- Kingsley-Hughes, Adrian & Kingsley-Hughes, Kathy, *Beginning Programming*, 1a. edición, Indianapolis, IN, Wiley Publishing, Inc., 2005.

- Penrose, Roger, *La mente nueva del emperador*, 2ª. edición en español, México, DF, Fondo de Cultura Económica, 2002.

- _____ Quantum Mechanics en *Enciclopedia Británica*, 16ª. edición, Chicago, IL. Enciclopedia Británica, Inc., 1948.

- Wilbert, Ken, *Cuestiones cuánticas*, España, Kairos, 12ª. Edición, 1987

DOCUMENTOS EN INTERNET

- Hardesty, Larry, *Proving quantum computers feasible,* MIT News Office, http://web.mit.edu/newsoffice/2012/proving-quantum-computers-feasible-1127.html Consultado 16.12.2012

- Coffeen Holton, William, *quantum computer,* Encyclopedia Britannica Online, http://www.britannica.com/EBchecked/topic/746092/quantum-computer Consultado 25.01.2013

- *Redes de comunicaciones,* Güimi, http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-RCnode59.html Consultado: 02.12.2012

- *Criptografía Cuántica - Conceptos de Criptografía*, Textos científicos, http://www.textoscientificos.com/criptografia/quantica Consultado: 02.12.12

- Triana, Harvey, *Algunos Procedimientos Visual Basic para Codificar y Decodificar Información*, VeXPERT, http://vexpert.mvps.org/articles/vbEncrypt.htm Consultado: 01.12.2012

- Singh, Simon, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, New York, NY, Doubleday of New York, 1999.