Computación Cuántica
Un Nuevo Reto para la Seguridad Informática

Reyes Alvarez, Marcos Fernando.
mreyes@unisangil.edu.co
Unisangil

Resumen—La computación cuántica se puede interpretar como la palabra clave en el futuro de la computación y la tecnología, por medio del uso de los fotones con sus características como la superposición y el entrelazamiento, para almacenar y enviar información a través de los qubits, estableciendo los canales de comunicación necesarios y brindando nuevos métodos para proteger la información, pero sin olvidar las potenciales amenazas a la seguridad de la información que pueden poner en riesgo la información.

Índice de Términos—Computación Cuántica, Superposición, Entrelazamiento, Qubits

I. INTRODUCCIÓN

A cerca de la computación cuántica ya existe un modelo teórico producto de la investigación de varios años. Allí se incluye la ruptura de algunos paradigmas como la criptografía tradicional, y se abre la puerta a la criptografía cuántica, debido a que una computadora cuántica podrá ejecutar muchas operaciones por segundo comparado con la computadora tradicional, haciendo más rápidos los procesos matemáticos, lo cual es la base de los algoritmos actuales, que con su estructura lógica podrán hacer que romper un contenido cifrado con ciertas características de seguridad sea cuestión de meses y años. Con la computación cuántica esos mismos procesos se podrán realizar en cuestión de segundos.[1] Según la física cuántica un mismo objeto, una molécula, un átomo podría estar en dos lugares distintos a la vez, pero así mismo es bastante interesante analizar como 2 partículas en diferentes partes del universo podrían estar entrelazadas; pero todo eso es una incertidumbre. No podemos conocer con precisión todas las características de una partícula subatómica, además las partículas no tienen una posición ni una trayectoria definidas, sino que se hallan en distintos lugares a la vez con distintas probabilidades, a lo cual se le llama superposición, pero al intentar medir con precisión las características de un objeto cuántico, su estado será radicalmente distinto del que tenía antes de la medición, lo cual es una característica intrínseca de la naturaleza cuántica, siendo un comportamiento que abre la posibilidad de fenómenos interesantes, como por ejemplo el entrelazamiento que se puede dar entre una pareja de partículas, ocasionando que cuando algo modifica el estado de una de las dos partículas, automáticamente modifica el estado de la otra, y esa conexión especial se mantiene aún si las dos partículas se encuentran a los dos extremos de una galaxia. El mismo Einstein definía el entrelazamiento como "acción fantasmal a distancia". El entrelazamiento se puede interpretar como un intercambio de información entre dos partículas, según Vlatko Vedral. [2] (Profesor de física de la universidad de Oxford).

Si se pudiese hacer que un objeto grande estuviera en varios estados a la vez entonces se podrían crear los denominados ordenadores cuánticos, haciéndolo mucho más eficiente que un ordenador actual. Gracias a la superposición un qubit puede tener dos o más valores al mismo tiempo, lo cual permitiría realizar múltiples tareas a la vez, como descifrar rápidamente los factores de un número grande, buscar en listas muy extensas, o simular con gran detalle sistemas complejos como el clima. Pero una consideración a tener en cuenta con el ordenador cuántico sería el aislamiento, debido a que cualquier perturbación puede alterar su comportamiento. [3]

A. Orígenes de la Teoría Cuántica

"Si he visto más lejos, ha sido por subirme a hombros de gigantes" Isaac Newton.

TABLA I
REVOLUCIÓN CUÁNTICA: DE NEWTON A EINSTEIN

Personaje	Hallazgo
Isaac Newton (1642 - 1727)	**(1687)** - Ley de la Gravitación Universal
James Clerk Maxwell (1831 - 1879)	**(1873)** - leyes de la inducción electromagnética y de los campos de fuerza
Max Planck (1858-1947)	**(1900)** - Ley de Planck Premio Nobel (1918)
Albert Einstein (1879 - 1955)	**(1905)** - Dualidad Onda Partícula Premio Nobel de Física (1912)
Niels Bohr (1885 - 1962)	**(1922)** - Explicó la Estructura del átomo Premio Nobel de Física
Erwin Schrödinger (1887 - 1961)	**(1926)** - Ecuación de Schrödinger Premio Nobel de física (1933)
Louis de Broglie (1892 - 1987)	**(1929)** - Dualidad Onda-Corpúsculo Premio Nobel Física (1929
Gordon Moore (1929 -)	**(1965)** - Ley de Moore
Richard Feynman (1918 - 1988)	**(1985)** - Teoría de los Partones Premio Nobel de Física (1965)
Peter Shor (1959 -)	**(2001)** - Algoritmo de Shor

FUENTE: AUTORÍA PROPIA

El origen de la teoría cuántica data del periodo comprendido entre 1900 y 1905, teniendo como protagonista a Albert Einstein y Max Planck. [4] En diciembre de 1900 planck introdujo el cuanto de energía con el fin de describir las propiedades espectrales de la radiación, mediante un proceso de distancias discretas o cuantización (electrones que giran alrededor del núcleo a ciertas distancias específicas) aplicado a la materia. Einstein también descubrió que la luz no es una onda continua, sino que a veces se comporta como una partícula, lo cual llaman los físicos dualidad onda partícula, además descubrió que la luz se comporta como si viniera en pedazos, en trocitos, o en cuantos de luz (fotones), lo que le valió un premio nobel. [5]

B. Primera Revolución Cuántica

Newton por medio de varias ecuaciones matemáticas sencillas describió y predijo el movimiento de los planetas, descubrió que el mundo es fundamentalmente predecible. [6] James Clerk Maxwell demostró que la electricidad y el magnetismo podían resumirse con varias ecuaciones matemáticas, ecuaciones que tuvieron un gran impacto sobre el desarrollo tecnológico del siglo XX. [7] En 1923 Niels Bohr comenzó a complementar el modelo cuántico explicando la estructura del átomo por medio de ecuaciones sencillas, explicó las propiedades de los átomos mediante la mecánica cuántica (cuantización). [8] El físico francés Louis de Broglie demostró que las órbitas atómicas pueden explicarse asumiendo que los electrones también pueden comportarse como ondas. [9] Erwin Schrödinger en 1925 formuló la ecuación que lleva su nombre, sentando las bases de una teoría completa de la mecánica cuántica, dando a los científicos una receta universal para entender todos los fenómenos cuánticos anteriores, y les proporcionó una forma sistemática de explorar el mundo atómico para obtener nuevos e inexplorados efectos cuánticos. [10] *(Ver Tabla I)*

[10] Mientras un objeto cuántico no es medido ni se interactúa con su entorno, típicamente no tiene una posición definida, sino que está a la vez en muchas posiciones, como si pudiera ser y hacer varias cosas al mismo tiempo, a lo que se le llama la superposición cuántica. [11] En la paradoja Einstein, Podolsky y Rosen demostraron que ciertas combinaciones de superposiciones de partículas podrían combinarse de una forma extraña, ilógica e imposible de explicar según la mecánica clásica. [12]

Stephen Hawking. "La diferencia básica entre la física clásica y la cuántica es que en la física clásica se puede predecir tanto la posición como la velocidad de las partículas, mientras que en la teoría cuántica no se puede predecir ninguna de las dos." [13]

C. Segunda Revolución Cuántica

La segunda revolución cuántica cuenta con dos características principales 1. Capacidad de controlar la rareza del mundo cuántico incluidas la superposición y el entrelazamiento, 2. Es el auge de la era de la información, ahí llega la información cuántica o IQ. [14]

En 1985 el físico americano Richard Feynman, hablaba de la posibilidad de que los ordenadores funcionaran por principios cuánticos. Introdujo la teoría de los partones, hipotéticas partículas localizadas en el núcleo atómico, que daría pie más tarde a la introducción del moderno concepto de quark. Su aporte a la física teórica ha quedado almacenado en títulos tales como Quantum. [15]

La tecnología actual ya se está aproximando a los límites de la información cuántica, y nuestros transistores se acercan al tamaño de un bit cuántico, o qubit, a lo cual en un principio se asoció a la llamada ley de Moore en honor al fundador de Intel, y se esperaba que en los siguientes 20 años los transistores que son el corazón de los dispositivos informáticos se acercaran al tamaño de un único átomo. [16]

Existe una tesis fundamental muy importante en la informática llamada la tesis moderna de Church/Turing que dice que todos los ordenadores clásicos normales son básicamente equivalentes, y no es que funcionen a la misma velocidad, sino que siguen las mismas normas, se comportan de forma similar, y si se intenta realizar una tarea con un portátil y después se intenta hacer lo mismo con otro ordenador, se comportará prácticamente de la misma forma. [17]

Stephen Hawking "los ordenadores cuánticos se basan en el hecho de que el estado cuántico de la memoria de un ordenador contiene mucha más información que sus descripciones clásicas". [13]

D. Aplicación de la Computación Cuántica

La computación cuántica presenta diferentes aplicaciones que ya se están implementando, y otras que serán aplicadas a futuro, tal como se mencionan en la Tabla II.

TABLA II
APLICACIONES DE LA COMPUTACIÓN CUÁNTICA

Área, Función o Clasificación	Aplicaciones
La Criptografía	Aseguramiento los resultados electorales en Suiza. Mediante la criptografía vinculando la fibra óptica que conectaba el lugar donde se contaron las papeletas con el lugar donde estaban los ordenadores del proceso electoral. [18]
Cuántica	La codificación de información confidencial (debe ser tan sólida que nadie pueda romperla, pero a su vez genera una barrera para cuando se deben analizar delitos informáticos, y se encuentra la información cifrada. Shor) [27]
La Tele Transportación Cuántica	El traslado de la información cuántica desde un punto a hacia b. la tele transportación cuántica es posible por el entrelazamiento de dos fotones para transmitirle información del uno al otro. [19]
Simulación de Sistemas Cuánticos	Un simulador de un sistema de vuelo. [20]
	Simulación de los átomos de un fármaco para indicar cómo prepararlo, y cómo interactuará con otras sustancias químicas. [22]
El Diseño de Nuevos Súper Conductores	Dirección de trenes de levitación magnética. [21]
Búsqueda, Identificación y Detección	Identificación el mercurio en el pescado. [23]
	Búsqueda del plomo en los juguetes. [24]
	Detección de bombas. [25]
Sensores	Realización de sensores más sólidos, más precisos, más sensibles, y si se pueden compactar se podrán usar ampliamente en el entorno medioambiental. [26]

FUENTE: AUTORÍA PROPIA.

E. Seguridad de la información y la Computación Cuántica

El auge de las tecnologías, más específicamente con las computadoras, celulares, tablets, entre otros, ha sido de un gran impacto para la humanidad en los últimos años, lo cual ha traído muchos beneficios a la sociedad facilitando la vida a millones de personas, permitiendo realizar actividades que en el pasado eran tediosas y lentas, pero que en la actualidad se pueden desarrollar en unos pocos minutos y con una relativa facilidad.

Como una de esas innovaciones podemos identificar la computadora cuántica, aunque aún está en prototipos de laboratorios y pruebas científicas, ya es una realidad que en cualquier momento empezará a inundar el mercado tecnológico mundial, y en general es algo espectacular, poder presentar al mundo un avance tan interesante, que sea producto de la evolución y el estudio de muchos años y muchas mentes brillantes que han realizado valiosos aportes. Pero en este punto es donde empiezan las preguntas, cuánta similitud puede haber frente al lanzamiento de la computadora tradicional, ya que los mayores esfuerzos fueron para ponerla a funcionar, pero se descuidó la seguridad y ya cuando todo el mundo tenía implementada su tecnología, fue cuando empezaron a surgir las diferentes amenazas producto de los errores en el desarrollo, configuración y funcionamiento, que con

el paso del tiempo se convirtieron en vectores de ataque de piratas informáticos para cometer gran variedad de delitos contra las personas.

En el caso del desarrollo de un ordenador cuántico, como amenaza puede descifrar muchos de los códigos de encriptación usados hoy en día, incluidos los que se usan en los satélites, en los bancos, en las tarjetas de crédito, y para las comunicaciones de seguridad. Aunque un ordenador cuántico podría develar mensajes secretos, los efectos cuánticos también podrían usarse para crear los códigos secretos mundiales más seguros, códigos cuánticos, y ofrecer una forma súper secreta de mantener la confidencialidad. Paradójicamente algo que puede fortalecer la seguridad en el mundo cuántico, es el uso de métodos clásicos de seguridad, pero que mezclados con la tecnología moderna, puedan brindar mayores niveles de aseguramiento de la información y las aplicaciones. [28]

En la comunicación en la nube se podrá utilizar la computación cuántica para transportar información confidencial a través de largas distancias, utilizando los fotones para codificar la información de los qubits, aprovechando la cualidad de los múltiples estados, de forma que nadie conozca cual ha sido el estado inicial y solo el usuario que está realizando el procedimiento lo conozca y así poder asegurar la información, lo cual en teoría hasta el momento es algo casi perfecto, [29] pero que debe mantenerse la atención posible en el mismo para no dar lugar a errores que permitan con el tiempo a un atacante capturar el estado inicial y poder empezar a decodificar la información. Actualmente algunos físicos e investigadores como David Bacon [30] buscan permanentemente diferentes usos que se puedan dar a la computación cuántica, buscando innovaciones que revolucionen el tiempo y espacio de formas que nunca nadie pudiera haber imaginado [31].

Dentro de la computación cuántica se debe trabajar de la mano con individuos que tengan conocimiento y cercanía del hacking, para que a medida que se va avanzando en el desarrollo de diferentes proyectos con tecnología cuántica, se vaya teniendo en cuenta paralelamente la seguridad de la información. [32]

F. Algunas Innovaciones

A continuación se presenta una tabla con algunas de las innovaciones que han venido apareciendo en cuanto a la computación cuántica.

TABLA III
ALGUNAS INNOVACIONES DE LA COMPUTACIÓN CUÁNTICA

INNOVACIONES	
Aspecto/Elemento	**Descripción**
Chip de Silicio que genera sus propios fotones	Un equipo de investigación internacional dirigido por la Universidad de Bristol, en Reino Unido, ha generado y manipulado por primera vez partículas individuales de luz –o fotones-, en un chip de silicio. [33]. Un conjunto de científicos e ingenieros, dirigidos por el doctor Mark Thompson construyeron un chip capaz de exponerse al ataque directo de un rayo láser. [34]
La Tecnología Cuántica llega a la vida de las personas	La computación cuántica se presenta como la gran promesa para seguir construyendo equipos más veloces. A diferencia de un ordenador tradicional que se ejecuta en bits binarios, los qubits cuánticos pueden ser 0 y 1 a la vez, lo que facilita un aumento importante en la velocidad de procesamiento. Fundamental para acelerar la búsqueda en bases de datos o el aprendizaje automático. Sin embargo, mientras los bits binarios se basan en transistores de silicio de confianza, los expertos aún deliberan sobre el mejor material para los equipos cuánticos. [35]
IBM avanza hacia el Primer computador Cuántico	Investigadores de IBM han dado a conocer dos avances importantes hacia la realización de un ordenador cuántico de uso práctico. [36] Han mostrado la capacidad de detectar y medir simultáneamente los dos tipos de errores cuánticos que se producirían en cualquier ordenador cuántico real. También han mostrado un nuevo diseño de circuito que -afirman- es la única arquitectura física que podría ser escalable a mayores dimensiones con éxito. Los ordenadores cuánticos prometen abrir nuevas posibilidades en el campo de la optimización y simulación que, simplemente, hoy día no son alcanzables. Esto es por su capacidad de computación. Por ejemplo, un ordenador cuántico de sólo 50 bits

	cuánticos (qubits) superaría a cualquier combinación de supercomputadoras TOP500 actual en capacidad computacional. [37]
"Internet Cuántica"	"Las computadoras cuánticas podrían comunicarse en principio entre sí mediante el intercambio de fotones individuales para crear una Internet cuántica" [38]. Un equipo de científicos liderados desde la Universidad Autónoma de Barcelona ha desarrollado un material que guía y transporta el campo magnético de forma parecida a como una fibra óptica lo hace con la luz o una manguera con el agua. El prototipo de 'fibra magnética' mide 14 centímetros, pero puede implementarse a cualquier escala, incluida la nanométrica. Innovación que acerca más a la aplicación en el mundo del internet cuántica [39]

FUENTE: AUTORÍA PROPIA.

G. ¿Máquinas Conscientes? ¿Inteligencia Artificial?

Algunos títulos relacionados a la computación cuántica [40] suenan fabulescos, salidos de las mejores películas de ciencia ficción de Hollywood, pero esta vez el sueño es tan real que parece mentira. Cuando se escucha hablar de la conciencia en una máquina, de un cerebro artificial, o de un pensamiento cuántico, sencillamente es un apasionante mundo del conocimiento que viene en camino por descubrir, que abre las puertas de la curiosidad y el reto por superar las barreras de la inteligencia humana. Investigaciones sustentan que las máquinas conscientes son el siguiente reto tecnológico, con la premisa de poder imitar el funcionamiento del cerebro humano, quizás puedan llegar a simular lo que puede ser un proceso realizado por la conciencia, o simular algo aproximado a los sentimientos y las emociones. [41]

Según estudios científicos, la inteligencia surge como una consecuencia de la conciencia, por lo tanto para alcanzar una Inteligencia Artificial [42] lo más aproximada a la realidad posible, se requiere tener un alto nivel de simulación de la conciencia. En cuanto a la simulación de un cerebro artificial se dice que para que en algún momento se trataran de simular sentimientos y emociones debería construirse la cabeza y el cuerpo artificiales para que dicho experimento pudiese ser realizado con más probabilidad de éxito. "la teoría de que la conciencia se comporta como las partículas cuánticas, al igual que algunas de las funciones de la biología molecular son a todas luces procesos cuánticos". [43] Lo anterior sería una explicación al estudio de la conciencia en animales como por ejemplo monos y perros, donde los científicos debaten si las respuestas de estos animales se deben al simple instinto, o a experiencias subjetivas humanas como la alegría, la ira, el dolor, los deseos o las intenciones. La respuesta a estos interrogantes brindará una mayor aproximación al avance de la simulación cuántica de las funciones cerebrales. *"El universo está poblado de galaxias y el cerebro de neuronas. La sensación de totalidad es común al cerebro y a universo"*. [44].

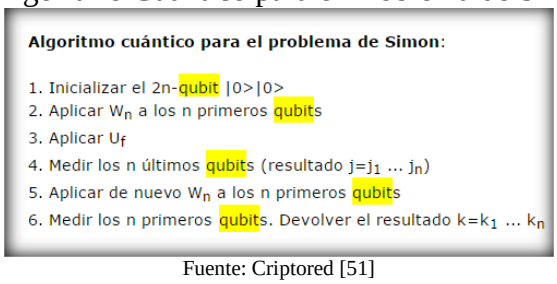
En cuanto al pensamiento cuántico, la inteligencia artificial y temas afines, se debe tener en cuenta la robótica, ya que según un trabajo teórico hispano-austríaco, los robots cuánticos serán más creativos y responderán más rápido a los cambios en su entorno, dando como resultado una nueva generación que revolucionará el mundo tecnológico por completo [45]. Por ejemplo, por primera vez un software instalado en un superordenador, el Eugene Goostman (que simula a un niño de 13 años y que fue desarrollado en San Petersburgo, Rusia), ha superado la Prueba de Turing 2014, celebrada por la Royal Society en Londres. Lo cual significa un gran avance en cuanto a la robótica y la inteligencia artificial y aproxima cada vez más este nuevo paradigma al mundo actual. [46].

Las casas domóticas son otro vector que viene a mezclar la robótica, la inteligencia artificial y además vinculará a la computación cuántica dentro de su accionar. "Desde cualquier ordenador conectado a Internet o desde cualquier Smartphone se podrá cambiar el estado de los dispositivos de forma remota, como variar la intensidad de una luz o bajar una persiana. También se podrá visualizar los eventos que se han producido en la casa, por ejemplo cuando alguien activa un sensor de presencia o ver en qué momento se ha encendido la calefacción", explica Lozano-Tello. [47].

H. Criptografía Cuántica

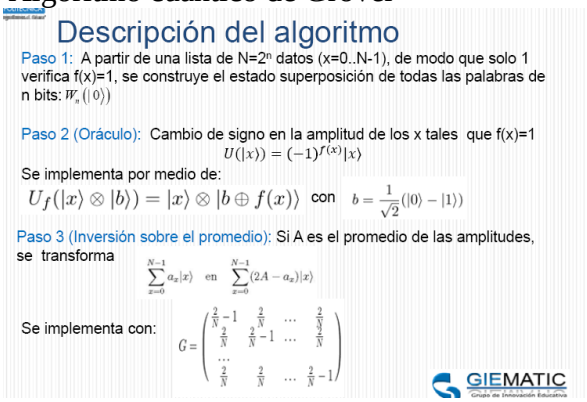
Dentro de la criptografía cuántica ya se han venido trabajando algunos algoritmos criptográficos, a partir de las debilidades de la criptografía clásica y las bondades de la mecánica cuántica, para poder brindar mejores soluciones de seguridad a las comunicaciones. Algunos de estos algoritmos cuánticos que han surgido en los últimos años son los siguientes

- Algoritmo Cuántico para el Problema de Simón.



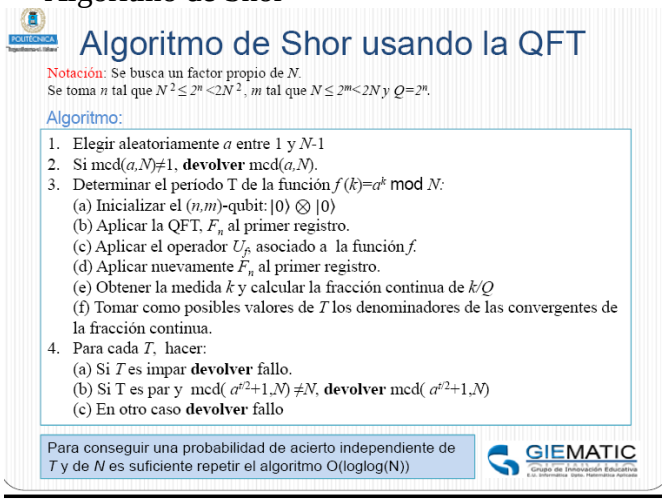
Fuente: Criptored [51]

- Algoritmo cuántico de Grover



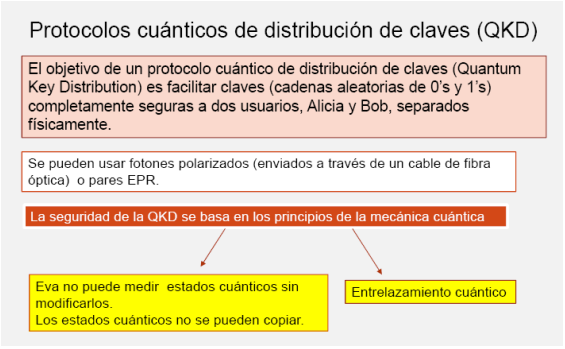
Fuente: Criptored [51]

- Algoritmo de Shor



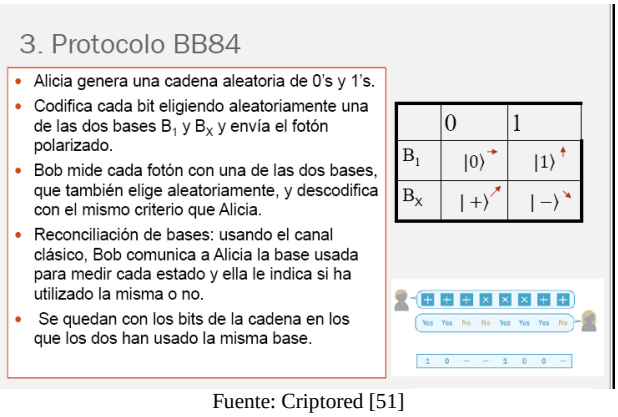
Fuente: Criptored [51]

Hallazgos como los descritos anteriormente, donde se proponen nuevos algoritmos que se inmiscuyen dentro de la criptografía cuántica, son los que han dado pie a las nuevas propuestas y protocolos de seguridad relacionados a la computación cuántica. Tales como los protocolos cuánticos de distribución de claves (QKD).



Fuente: Criptored [51]

Este tipo de estudios y profundización de la criptografía y por ende la computación cuántica, han llevado a diferentes avances y logros que con el tiempo van a ir tomando más fuerza y se van a popularizar dentro de la sociedad como la nueva era de la tecnología, reemplazando de una forma secuencial y cuidadosa lo que hoy es la criptografía tradicional, en busca de soluciones a los problemas que hoy en día aquejan a la seguridad de la información.



Fuente: Criptored [51]

I. Visión desde la perspectiva de la seguridad informática

Así como en todas las áreas de la tecnología, la telefonía también tendrá diferentes avances que modernizarán el mundo, pero se deben tener en cuenta algunos aspectos de seguridad que

mezclados con la computación cuántica podrán ser nuevos campos donde los delincuentes informáticos se fortalezcan paralelamente [48]. Por ejemplo, en cuanto a los Smartphone se tiene que los Malware de la nueva era empiezan a ejecutar aplicaciones automáticamente, arrojar invitaciones y ventanas pretendiendo que los usuarios en un descuido acepten y se contaminen los dispositivos, por eso ya se está trabajando en que los dispositivos comparen las acciones del teléfono con los movimientos de la mano del usuario, de forma que cuando el celular ejecute acciones sin presentar un registro de movimiento, automáticamente se disparen alertas antimalware que bloqueen el dispositivo y mitiguen la amenaza. [28] Pero acá se empiezan a trenzar las incertidumbres de qué sucederá cuando las técnicas de los atacantes también incluyan programación cuántica, y usen los mismos conocimientos para poder evadir los controles de seguridad, por decir, si se hace una aplicación inteligente para bloquear malware, ¿podrá darse el momento en que también los atacantes falsifiquen estos controles y engañen a los usuarios para poderlos hackear?. Por ejemplo Twitter revela dónde vive una persona, incluso con la geolocalización desactivada [49]. Este tipo de innovaciones pese a presentar interesantes avances para la sociedad, también son potenciales vectores de ataque que se empiezan a abrir, ya que a una persona le podrán hacer seguimiento sin estar siquiera conectada a internet, ¿si no es un familiar o alguien cercano, entonces cualquier sospechoso podría obtener ese tipo de información y usarla para que fines? Y si tenemos métodos de cifrado y conexiones cuánticas irrompibles, como poder identificar que hay un intruso. Un nuevo teclado virtual permitirá escribir sin dispositivo físico. Este tipo de noticias son muy atractivas desde la perspectiva comercial y desde el consumismo e innovación tecnológica, pero surge nuevamente la inquietud acerca de la seguridad, como se puede asegurar que un intruso ahora sin tener el dilema de colocar un dispositivo físico, simplemente llegue a hackear la señal de ese teclado virtual y usarlo como keylogger dejando aún menos evidencias que un dispositivo físico. [50]

Cuando las teorías básicas de la comunicación cuántica, se empiecen a aplicar propiamente en una computadora o en un simulador de la conciencia humana, deberán existir tratados, conductos, "manuales", de cómo llegar a realizarlo, y los Cyber Adictos, en especial aquellos con perfil Black Hat estarán buscando las maneras de comprender absolutamente todo, y creando los manuales más allá del manual, que luego caerán seguramente en manos de los delincuentes informáticos, y así como los científicos construyeron un camino, los intrusos buscaran reconstruir el propio y generar nuevas amenazas.

A continuación se plantean algunos interrogantes que la ciencia irá respondiendo con el paso del tiempo, o quizás en algunos casos nunca se llegue a conocer la respuesta.

¿Podrá un concepto tan humano como la consciencia cobrar vida en los circuitos de algo inanimado como una computadora? ¿Es posible duplicar las funciones de un cerebro orgánico en una estructura artificial que se asemeje a la humana? ¿Podrán algunos procesos computacionales -radicalmente distintos de los que existen en el cerebro - generar propiedades mentales similares a las humanas? ¿Tendrán las inteligencias artificiales una "psicología"? Y de ser así, ¿sería ajena al ser humano? ¿Sabrán las máquinas lo que hacen, tendrán intenciones?

II. Conclusiones

La computación cuántica será el boom de las décadas venideras, siendo la mayor innovación y revolución informática de los últimos años, presentando un nuevo paradigma computacional, así como cuando se empezó a hablar de TCP/IP, pero esta vez con el reto de no dejar nada al azar, y estar en un permanente estudio y análisis de la ventajas como desventajas que podrá traer, incluyendo las diferentes medidas de control y mitigación ante las diversas amenazas que surgirán.

Pese a que ilustres investigadores a través de la historia pasada y presente, como Stephen Hawking mencionan sus premisas, como por ejemplo: "Los

principios de la informática cuántica se entienden perfectamente, lo difícil es su implementación, en la práctica". [12] Se puede inferir que es un arranque complicado, tedioso, nada fácil, pero seguramente cuando esa nave de nueva tecnología y conocimiento logre despegar, estará en una carrera directa, con obstáculos, pero con una experiencia y una visión panorámica lo suficientemente buena para superarlos y continuar hacia la meta.

Una de las premisas del ordenador cuántico es que requiere mantener las superposiciones cuánticas para que funcione correctamente, lo cual ha sido objeto de estudio, y seguramente se irán publicando diferentes teorías científico informáticas acerca de las mismas, pero como se ha mencionado anteriormente, no solo los científicos van a tener acceso a esta información, sino también, la sociedad en general, incluyendo a los delincuentes informáticos, los cuales van a tener como reto poder encontrar las falencias dentro de esas implementaciones de la superposición cuántica, buscando identificar los patrones de organización de las partículas, o incluso seguir el mismo camino que la ciencia seguirá para controlarlos, teniendo en cuenta que dentro de las técnicas de hacking se encuentran algunas como la suplantación de la identidad o la ingeniería social, que también se irían adaptando a su nuevo ambiente para seguir siendo aprovechadas.

La segunda revolución cuántica consiste en que hoy en día seamos capaces de manipular sistemas cuánticos individuales, moléculas individuales, átomos individuales, o fotones individuales. Hasta el momento después de la primera revolución cuántica, se podían manipular conjuntos, por ejemplo un láser que produciría miles de millones de fotones, y que hoy se puedan manejar quantos individuales, abre una nueva e inmensa área para el desarrollo tecnológico, pero igual queda la inquietud que pese a ese gran avance que puede significar, nada nos asegura que los intrusos lleguen a obtener el mismo conocimiento y sacar las mismas conclusiones para seguir haciendo de las suyas.

En la teoría, con la criptografía cuántica es prácticamente imposible husmear en la transmisión sin ser descubierto, a lo que se le puede llamar el efecto observador ruidoso, es como si se estuviera en una fiesta escuchando la conversación de la pareja de al lado, sabrían al instante, sin mirar siquiera que les estaban oyendo. ¿Y si los hackers llegaran a encontrar la forma de poderlo hacer sin que la víctima lo note, así como el man in the middle?

En la criptografía clásica se piensa que el sistema es seguro porque el supuesto fisgón no puede resolver un difícil problema informático. En la criptográfica cuántica no se puede descifrar un código criptográfico cuántico a menos que se descifren las leyes de la física. La pregunta es, ¿qué nos asegura que los delincuentes informáticos no lo lograrán por su sed de vulnerar los sistemas de información?

RECONOCIMIENTO

Agradecimientos del autor al Departamento de Investigaciones y a la Facultad de Ingeniería de Sistemas de la Fundación Universitaria de San Gil Unisangil, por su apoyo en el proceso investigativo.

REFERENCIAS

[1]"La computadora cuántica: los qubits", YouTube, 2016. [Online]. Available: http://www.(URL) [Accessed: 21- Mar- 2016].

[2]V. Vedral, Decoding reality. Oxford: Oxford University Press, 2010.

[3]R. cuántico, "Redes - La incertidumbre del universo cuántico, Redes - RTVE.es A la Carta", RTVE.es, 2011. [Online]. Available: http://www.(URL)/ [Accessed: 23- Mar- 2016].

[4]"Radiación del cuerpo negro - Hipótesis de Planck", Uco.es, 2016. [Online]. Available: http://www.uco.es [Accessed: 21- Mar- 2016].

[5]J. Sánchez Ron, "Planck, Einstein y los orígenes de la física cuántica", Arbor, vol. 167, no. 659-660, pp. 423-436, 2000.

[6]T. Broadbent, D. Whiteside and I. Newton, "The Mathematical Papers of Isaac Newton. I. 1664-1666", The Mathematical Gazette, vol. 52, no. 379, p. 59, 1968.

[7]A. Mott, "James Clerk Maxwell", Phys. Bl., vol. 21, no. 5, pp. 205-207, 1965.

[8]"Niels Bohr: Collected Works. Volume 7: Foundations of Quantum Physics II (1933-1958) Niels Bohr Jorgen Kalckar", Isis, vol. 90, no. 1, pp. 143-144, 1999.

[9]"Biografía de Louis de Broglie", Biografiasyvidas.com, 2016. [Online]. Available: http://www.(URL). [Accessed: 21- Mar- 2016].

[10]X. Qian, B. Little, J. Howell and J. Eberly, "Shifting the quantum-classical boundary: theory and experiment for statistically classical optical fields", Optica, vol. 2, no. 7, p. 611, 2015.

[11]"Biografía de Erwin Schrödinger", *Biografiasyvidas.com*, 2016. [Online]. Available: http://www.(URL). [Accessed: 21- Mar- 2016].

[12]R. Schlegel, "The Einstein-Podolsky-Rosen Paradox", Am. J. Phys., vol. 39, no. 4, p. 458, 1971.

[13]"Stephen Hawking: a life in science", Choice Reviews Online, vol. 40, no. 07, pp. 40-4063-40-4063, 2003.

[14]"Revolución Cuántica - documental online", *Ver-documentales.net*, 2016. [Online]. Available: http://www.(URL). [Accessed: 23- Mar- 2016].

[15]"Biografía de Richard Philips Feynman", *Biografiasyvidas.com*, 2016. [Online]. Available: http://www.(URL). [Accessed: 23- Mar- 2016].

[16]"La Ley de Moore camina hacia su muerte", abc, 2016. [Online]. Available: http://www.(URL) [Accessed: 23- Mar- 2016].

[17]J. Copeland, "The Church-Turing Thesis", NeuroQuantology, vol. 2, no. 2, 2007.

[18]"Criptografía cuántica para proteger el recuento electoral » Teleobjetivo", *Teleobjetivo.org*, 2016. [Online]. Available: http://www.(URL). [Accessed: 23- Mar- 2016].

[19]"La NASA logra la teleportación cuántica a la distancia récord de 25 kilómetros", *ABC.es*, 2016. [Online]. Available: http://www.(URL) [Accessed: 23- Mar- 2016].

[20]R. T21, "Crean un simulador cuántico que permite fenómenos físicos imposibles", *Tendencias 21. Ciencia, tecnología, sociedad y cultura*, 2016. [Online]. Available: http://www.(URL) [Accessed: 23- Mar- 2016].

[21]E. Arcos and I. Berazaluce, "Superconductividad para trenes de levitación magnética - Cooking Ideas", *Cooking Ideas*, 2011. [Online]. Available: http://www.(URL) [Accessed: 23- Mar- 2016].

[22]C. imposibles, "Científicos españoles inventan un simulador cuántico que recrea fenómenos físicos imposibles - RTVE.es", *RTVE.es*, 2014. [Online]. Available: http://www.(URL) [Accessed: 26- Mar- 2016].

[23]"Validación de la metodologia para el analisis de mercurio en agua tratada y cruda, y estandarizacion del analisis de mercurio en pescados por el metodo de absorcion atomicavapor frio para el laboratorio de analisis de aguas y alimentos de la universidad tecnológica de pereira.", *Universidad Tecnológica de Pereira*, 2016. [Online]. Available: http://www.(URL) [Accessed: 26- Mar- 2016].

[24]"Peligro por la presencia de plomo en algunos juguetes y joyas de juguete que se regalan en las fiestas - Especiales CDC - CDC en Español", *Cdc.gov*, 2016. [Online]. Available: http://www.(URL) [Accessed: 26- Mar- 2016].

[25]P. Gómez-Esteban, "Cuántica sin fórmulas - El detector de bombas de Elitzur-Vaidman - El Tamiz", *Eltamiz.com*, 2010. [Online]. Available: http://www.(URL) [Accessed: 26- Mar- 2016].

[26]"Sensores cuánticos biocompatibles — Noticias de la Ciencia y la Tecnología (Amazings® / NCYT®)", *Noticias de la Ciencia y la Tecnología (Amazings® / NCYT®)*, 2016. [Online]. Available: http://www.(URL) [Accessed: 27- Mar- 2016].

[27]"FayerWayer", *fayerwayer*, 2016. [Online]. Available: http://www.(URL). [Accessed: 27- Mar- 2016].

[28]C. Abajo and C. Abajo, "Un antiguo sistema de cifrado podría proteger de los ordenadores cuánticos", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL). [Accessed: 26- Mar- 2016].

[29]S. Científicas, "Seguridad para la futura computación cuántica en la 'nube'", *Agenciasinc.es*, 2012. [Online]. Available: http://www.(URL). [Accessed: 26- Mar- 2016].

[30]X. Yuan, S. Assad, J. Thompson, J. Haw, V. Vedral, T. Ralph, P. Lam, C. Weedbrook and M. Gu, "Replicating the benefits of Deutschian closed timelike curves without breaking causality", *npj Quantum Information*, vol. 1, p. 15007, 2015.

[31]P. Pérez, "India identifica a 540 millones de ciudadanos mediante el escaneo de iris", *Tendencias 21. Ciencia, tecnología, sociedad y cultura*, 2016. [Online]. Available: http://www.(URL)[Accessed: 26- Mar- 2016].

[32]P. Corrales, "Un software recurre a técnicas de hackeo para reforzar la seguridad de sitios web", *Tendencias 21.*

Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL). [Accessed: 26- Mar- 2016].

[33]V. Moret Bonillo, "Principios Fundamentales de la Computación Cuántica", *LIDIA Laboratorio de Inteligencia Atificial*, 2016. [Online]. Available: http://Principios Fundamentales de la Computación Cuántica. [Accessed: 26- Mar- 2016].

[34]P. Pérez, "Avance en computación cuántica: Crean un chip de silicio que genera sus propios fotones", *Tendencias 21. Ciencia, tecnología, sociedad y cultura*, 2016. [Online]. Available: http://www.(URL) [Accessed: 27- Mar- 2016].

[35]P. Corrales, "La tecnología cuántica llega a la vida cotidiana", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL) [Accessed: 16- Mar- 2016].

[36]R. T21, "IBM anuncia dos importantes avances hacia la fabricación del ordenador cuántico práctico", *Tendencias 21. Ciencia, tecnología, sociedad y cultura*, 2016. [Online]. Available: http://www.(URL) [Accessed: 27- Mar- 2016].

[37]J. Kelly, R. Barends, A. Fowler, A. Megrant, E. Jeffrey, T. White, D. Sank, J. Mutus, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, I. Hoi, C. Neill, P. O'Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A. Cleland and J. Martinis, "State preservation by repetitive error detection in a superconducting quantum circuit", *Nature*, vol. 519, no. 7541, pp. 66-69, 2015.

[38]F. Pagliano, Y. Cho, T. Xia, F. van Otten, R. Johne and A. Fiore, "Dynamically controlling the emission of single excitons in photonic crystal cavities", Nature Communications, vol. 5, p. 5786, 2014.

[39]"Crean una fibra magnética equivalente a las fibras ópticas", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL). [Accessed: 27- Mar- 2016].

[40]J. Gómez, "La realidad cuántica revoluciona el mundo de la información", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL)[Accessed: 28- Mar- 2016].

[41]S. Moriello, "Las máquinas conscientes son el siguiente reto tecnológico", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL) [Accessed: 27- Mar- 2016].

[42]P. Corrales, "La Inteligencia Artificial abandona la supercomputadora para meterse en la Nube", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL)[Accessed: 28- Mar- 2016].

[43]E. Martínez, "La conciencia se perfila como un proceso cuántico", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL). [Accessed: 28- Mar- 2016].

[44]J. Leach, "La inmensidad del cerebro es similar a la del universo", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL)[Accessed: 28- Mar- 2016].

[45]"Los robots cuánticos serán más rápidos y creativos", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL) [Accessed: 28- Mar- 2016].

[46]R. T21, "Un software que emula a un niño de 13 años marca un hito en la historia de la informática", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL) [Accessed: 28- Mar- 2016].

[47]"Un software permite hacer una instalación domótica 'casera'", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL) [Accessed: 28- Mar- 2016].

[48]C. Abajo and C. Abajo, "Teléfonos que reconocen a su dueño por la forma de teclear", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL). [Accessed: 28- Mar- 2016].

[49]P. Corrales, "Twitter revela dónde vives, incluso con la geolocalización desactivada", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL) [Accessed: 28- Mar- 2016].

[50]P. Corrales, "Un nuevo teclado virtual permitirá escribir sin dispositivo físico", Tendencias 21. Ciencia, tecnología, sociedad y cultura, 2016. [Online]. Available: http://www.(URL)[Accessed: 28- Mar- 2016].

[51]"MOOC Crypt4you UPM", *Criptored.upm.es*, 2016. [Online]. Available: http://www.Criptored(URL). [Accessed: 24- May- 2016].

[52]V. Scarani, "Quantum Computing: A Gentle Introduction", Phys. Today, vol. 65, no. 2, p. 53, 2012.

Autor

Marcos Fernando Reyes Alvarez, Ingeniero de Sistemas Egresado de Unisangil, con Especialización en Seguridad Informática en la Universidad Pontificia Bolivariana, y Certificación como Auditor ISO 27001. Actualmente vinculado a Unisangil como docente cátedra y coordinador del semillero de seguridad informática Sigsu, el cual pertenece al grupo de investigación Hydra. Perito informático vinculado a la rama judicial como auxiliar de la justicia desde el año 2010, y trabajando como ingeniero contratista en diversos proyectos de desarrollo de software y prestación de servicios de ingeniería en diferentes empresas. Contacto: markfdo@hotmail.com