Revista de Administración Pública

INAP

Tecnología cuántica y Ciberseguridad

Salvador E. Venegas Andraca

Resumen: En la tecnología cuántica, campo del conocimiento en que se conjugan la física, la matemática, la ciencia computacional y la ingeniería, buscamos entender cómo la física cuántica (la física de lo tremendamente pequeño) se puede utilizar para incrementar dramáticamente nuestra capacidad de recolección, procesamiento, transmisión y almacenamiento de la información.

En este artículo se presenta una introducción sucinta a las nociones fundamentales de la tecnología cuántica así como algunos de los retos y oportunidades más importantes que esta tecnología tiene en el ámbito de la ciberseguridad.

Palabras clave: tecnología cuántica, distribución cuántica de llaves, ciberseguridad, sensores cuánticos, internet cuántico.

Quantum Technology and Cybersecurity

In quantum technology, the field of knowledge in which physics, mathematics, computational science and engineering are combined, we seek to understand how quantum physics (the physics of the tremendously small) can be used to dramatically increase our collection capacity, processing, transmission and storage of information.

This article presents a succinct introduction to the fundamental notions of quantum technology as well as some of the most important challenges and opportunities that this technology has in the field of cybersecurity.

Keywords: quantum technology, quantum distribution of keys, cybersecurity, quantum sensors, quantum internet.

Fecha de recepción: 11 de febrero de 2019
Fecha de aceptación: 1 de abril de 2019

Revista de Administración Pública

INAP

Tecnología cuántica y Ciberseguridad

Salvador E. Venegas Andraca*

I. Introducción

La viabilidad y el progreso de la especie humana están ligados a la ciencia y la tecnología. Más aún, los productos de alto valor agregado que resultan de la investigación científica y tecnológica son fuente de riqueza material para las sociedades que inviertan capital humano y económico en estos quehaceres.

Las actividades del mundo moderno tienen una herramienta de trabajo común: la ciencia y la ingeniería de la computación. Esto se debe, entre otros motivos, a que:

- El empleo de plataformas computacionales poderosas es esencial para el análisis de datos experimentales. Ejemplo: estudio del genoma humano y redes complejas como Internet o las redes de suministro eléctrico.
- La eficiencia y precisión requeridas actualmente en transacciones financieras sería imposible de lograr sin sistemas computacionales avanzados.

* Doctor en Física y Maestro en Ciencias por la Universidad de Oxford. Maestro en Administración (MBA) e Ingeniero en Sistemas Electrónicos por el Tecnológico de Monterrey. Es fundador del cómputo cuántico en México y profesor-investigador en esa institución, en la que dirige el Grupo de Procesamiento Cuántico de la Información. Por sus contribuciones científicas, Salvador es miembro de la Academia Mexicana de Ciencias, Senior Member de la ACM y Premio Rómulo Garza 2015, además de miembro del Sistema Nacional de Investigadores y socio titular de la Somedicyt.

- El diseño de algoritmos sofisticados y el empleo masivo de hardware en la simulación de procesos y fenómenos naturales es una actividad cotidiana en la investigación actual. Ejemplo: estudio y predicción de estructuras tridimensionales de proteínas.

En este ir y venir de datos a través de computadoras y redes digitales, cuya expresión más refinada es Internet, hay un requerimiento esencial: la seguridad de la información, esto es, la existencia de métodos que garanticen lo siguiente [1]:

a) Que los remitentes y receptores de la información sean legítimos.
b) La integridad de la información, esto es, que en cualquier proceso, la información generada, enviada y recibida sea la misma.
c) Que cualquier desviación del comportamiento esperado en los incisos anteriores sea detectada y reportada a la brevedad.

A lo largo de la era digital, se ha creado una plétora de métodos para cumplir con las expectativas mencionadas en seguridad de la información, métodos que se pueden agrupar en dos rubros: autenticación (verificación de identidades) y criptografía (ocultamiento y develación de información). Algunos de estos procedimientos son muy sólidos en sus fundamentos matemáticos pero son difíciles de implantar, en tanto que otros tienen sus cimientos en conjeturas matemáticas, mas la implantación es más ágil que en el caso anterior.

Es en este contexto que la noción de tecnología cuántica toma relevancia en el mundo de la seguridad informática. Comencemos con una definición:

La tecnología cuántica es el conjunto de productos y procesos que, con el propósito de recolectar, transmitir, procesar y almacenar información, emplea objetos físicos cuyo comportamiento es descrito por la mecánica cuántica. A su vez, la mecánica cuántica es la rama de la física que estudia y describe el comportamiento de objetos muy pequeños, de tamaño atómico y subatómico [2].

En la tecnología cuántica, campo del conocimiento en que se conjugan la física, la matemática, la ciencia computacional

y la ingeniería, buscamos entender cómo la física cuántica (la física de lo tremendamente pequeño) se puede utilizar para incrementar dramáticamente nuestra capacidad de procesamiento de información, esto es, de cómputo y de comunicación de datos. Ejemplos de tecnología cuántica son la criptografía cuántica, las computadoras cuánticas y los sensores cuánticos.

La tecnología cuántica ha producido importantes avances teóricos y experimentales en la que participan universidades y centros de investigación de prestigio mundial (por ejemplo, Oxford, Cambridge, MIT, Caltech y el Instituto Max Planck, por ejemplo) y gobiernos (Canadá, China, EE.UU., Japón, Reino Unido y Singapur, entre otros).

Además, la tecnología cuántica es ya un mercado emergente cuyo valor se estima en cientos de miles de millones de dólares estadounidenses en el futuro cercano [3,4]. Algunos resultados sobresalientes de esta disciplina son:

- El diseño de algoritmos cuánticos como el algoritmo de Shor [5], capaz de factorizar números enteros largos en tiempo razonable usando una computadora cuántica; el algoritmo de Grover [6], el cual encuentra elementos en conjuntos desordenados de forma más eficiente que cualquier algoritmo posible ejecutado en computadoras convencionales; finalmente, el algoritmo de Childs *et al*, el cual atraviesa una red con conexiones aleatorias en menos tiempo que cualquier algoritmo diseñado anteriormente [7].
- En el caso de la transición del laboratorio a la industria, uno de los resultados más maduros de la tecnología cuántica es la criptografía cuántica comercial. El corazón de esta tecnología es el uso de sistemas cuánticos para generar claves de encriptamiento de datos, claves que gozan de una robustez en su generación y secrecía sin paralelo en el mundo de la criptografía no cuántica. Los sistemas comerciales de criptografía cuántica existen desde 2003 e ID Quantique [8] es la compañía de referencia en este rubro.
- Computadoras cuánticas comerciales. IBM [9] y D-Wave [10] han fabricado computadoras cuánticas que están ya disponibles en el mercado. IBM tiene

> varios modelos de computadoras cuánticas de propósito general, el acceso a estos ordenadores es vía Internet y puede ser gratuito o por pago, dependiendo de la capacidad de procesamiento requerida. Las computadoras cuánticas de D-Wave están hechas para resolver problemas de optimización (esto es, problemas cuya solución requiere conocer el valor máximo o mínimo de uno o varios parámetros) y se puede tener acceso a ellas vía compra directa o a través de Internet.

Por su capacidad disruptiva en capacidades científicas y nuevos mercados tecnológicos, la tecnología cuántica es una área observada y estudiada por organizaciones de alcance continental como el BID [11] y la Unión Europea [12], además de los países ya mencionados y otros.

En este artículo se presenta una introducción-reflexión sobre el desarrollo, uso y aplicaciones de tecnología cuántica en el contexto de la ciberseguridad nacional.

2. Tecnología cuántica y su relación con la ciberseguridad

De acuerdo con la Unión Internacional de Telecomunicaciones, la ciberseguridad se define como *el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno* [13].

Como se declara en la sección anterior, la tecnología cuántica es el conjunto de productos y procesos que, con el propósito de recolectar, transmitir, procesar y almacenar información, emplea objetos físicos cuyo comportamiento es descrito por la mecánica cuántica. Los objetos cuánticos, al ser utilizados como recursos tecnológicos, proveen a la humanidad de nuevas e inesperadas capacidades computacionales y de comunicación de datos. Por ejemplo, pueden ser empleados para desarrollar algoritmos poderosos [14] o para teletransportar información [15].

Las propiedades de la tecnología cuántica representan, simultáneamente, un reto mayúsculo y una oportunidad

excepcional para la ciberseguridad global y, en particular, la de nuestro país. En las siguientes líneas damos cuenta de algunos de resultados y tendencias más importantes de la tecnología cuántica en el ámbito de la ciberseguridad.

2.1 Criptografía cuántica.

Breve introducción a la criptografía

La criptografía puede definirse como la rama de la ciencia y la ingeniería dedicada al diseño e implantación de métodos para tener comunicaciones seguras, bajo el supuesto de que hay un tercer involucrado (un espía) que está interesado en leer nuestros mensajes [1]. Más aún, el tercer involucrado está dispuesto a invertir tiempo, capital humano y recursos financieros en lograr su cometido. Es costumbre utilizar los nombres de Alice y Bob para referirnos al emisor y receptor de un mensaje, en tanto que Eve es el nombre empleado para referirnos al espía.

Existen dos tipos de métodos criptográficos: simétricos y asimétricos.

- Los métodos simétricos, también conocidos con el nombre de criptosistemas de llave privada, son algoritmos que emplean el mismo conjunto de símbolos para encriptar (ocultar) y desencriptar (develar) información. En los métodos de llave privada, Alice y Bob tienen el mismo conjunto de símbolos, conjunto que es conocido solamente por ellos y que emplearán para ocultar y develar mensajes.
- Los métodos asimétricos, también llamados criptosistemas de llave pública, son algoritmos que emplean dos llaves para ocultar y develar datos, una privada (conocida sólo por Alice y Bob) y otra pública (esta llave la conoce todo mundo).

Como ejemplo de un criptosistema de llave privada, suponga que Alice desea enviar a Bob el mensaje **EL CULPABLE TIENE LLAVES** y que acordaron, tiempo atrás, emplear la clave **BHGCAL** para construir una llave privada.

Los pasos que Alice y Bob convinieron seguir, para la transmisión de cualquier mensaje, es el siguiente (conocido como el método de Vigenère):

a) Los espacios del mensaje que se encriptará son eliminados.
b) La llave de encriptación se genera yuxtaponiendo la palabra clave.
c) Las letras del mensaje y la llave de encriptación se alinean en columnas.

El resultado de estos incisos, con el mensaje **EL CULPABLE TIENE LLAVES** y la palabra clave **BHGCAL**, es el siguiente:

Mensaje	E	L	C	U	L	P	A	B	L	E	T	I	E	N	E	L	L	A	V	E	S
Llave	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G

d) Ahora, las letras del texto a encriptar son sustituidas por las letras que resultan del siguiente procedimiento:

- Seleccione una letra del texto a encriptar y la letra correspondiente de la llave de encriptación.
- En la Fig. (1), localice la letra que está en el cruce del renglón que corresponde a la letra del texto y la columna que corresponde a la letra de la llave.
- Sustituya la letra del mensaje por la letra de la Fig. 1 encontrada conforme el inciso anterior.

En nuestro ejemplo, el resultado es:

Mensaje	E	L	C	U	L	P	A	B	L	E	T	I	E	N	E	L	L	A	V	E	S
Llave	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G	C	A	L	B	H	G
Mensaje encriptado	**F**	**R**	**I**	**W**	**L**	**A**	**B**	**I**	**Q**	**G**	**T**	**S**	**F**	**T**	**K**	**N**	**L**	**L**	**W**	**L**	**Y**

Los protocolos de llave privada pueden ser muy poderosos. Si las llaves cumplen con: i) ser en verdad privadas (esto es, que se puede garantizar que son de la exclusiva propiedad de Alice y Bob); ii) generada aleatoriamente; iii) de tamaño al menos igual al mensaje que se desea encriptar y iv) utilizada sólo una vez, entonces es posible construir protocolos de criptografía de llave privada invencibles, esto es, protocolos para los que es imposible que un espía pueda recuperar

el mensaje enviado a partir del mensaje encriptado [16]. Empero, las condiciones que las llaves privadas deben cumplir son extremadamente difíciles de cumplir, de ahí que se haya buscado esquemas de criptografía alternativos, como los de llave pública.

Figura 1
Tabla del método de Vigenère

Texto \ Llave	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	U	V	W	X	Y	Z	V	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Distribución cuántica de llaves: una solución al problema de secrecía

En los métodos tradicionales de distribución de llaves privadas, la mayor dificultad a vencer es garantizar la secrecía de la llave, esto es, que la llave sea del conocimiento exclusivo de Alice y Bob. Las llaves distribuidas en medios impresos pueden ser fácilmente copiadas sin que Alice ni

Bob se enteren (esto fue, en buena medida, la ruina del código Enigma, protocolo de encriptación utilizado por el gobierno alemán durante la Segunda Guerra Mundial [17]). Lo mismo sucede con llaves distribuidas a través de medios eléctricos o electrónicos: telégrafo y télex antaño, hoy correos electrónicos, chats y cualquier tipo de mensajería digital, una llave que se distribuya por estos u otros medios es posible copiarla ***sin*** que los responsables/usuarios se percaten de esto.

Una pertinente acotación a lo anterior es que los medios digitales modernos encriptan los mensajes que se envían a través de sus plataformas. Whatsapp, por ejemplo, utiliza *end-to-end encryption*, un método criptográfico asimétrico que, con la tecnología disponible en la empresa, es difícil de vencer. Difícil mas no imposible pues *end-to-end encryption* adolece de los problemas que todo método asimétrico tiene, además de existir ya documentación técnica respecto de fallas en *end-to-end encryption* debidas a problemas de autenticación [18]. En consecuencia, la secrecía en la distribución de llaves privadas tampoco está garantizada por la tecnología contemporánea de mensajería electrónica.

En línea con estos esfuerzos, Charles Bennett y Giles Brassard publicaron en 1984 un método de generación de llaves privadas empleando sistemas cuánticos [19] conocido como el protocolo BB84. En esencia, el BB84 consiste en crear llaves privadas mediante la transmisión y medición de sistemas cuánticos. Ejemplos de estos sistemas cuánticos son los electrones y los fotones (los fotones son las partículas de las que se compone la luz). Una vez construida una llave privada a través del BB84, esta llave puede utilizarse en cualquier protocolo simétrico (AES o DES, por ejemplo [20]).

Las propiedades físicas de los sistemas cuánticos del BB84 permiten determinar, ***durante el proceso de construcción y distribución de una llave privada***, si hay un espía escuchando en el canal de comunicaciones cuánticas usado para dicho proceso. En caso de detectarse la presencia de un espía, el proceso de creación y distribución de la llave se interrumpe de inmediato, para después intentarlo nuevamente. Obsérvese que la detección de espías por parte del protocolo BB84 se hace mucho antes de que dicho agente intente tener acceso al mensaje encriptado.

En otras palabras, el mensaje a transmitir nunca se ve comprometido.

Con la llegada de la criptografía cuántica, la transmisión de datos tiene una nueva dimensión en seguridad pues la privacidad de la información está ahora vinculada a las propiedades físicas de los objetos con los que construimos llaves privadas.

Además del BB84, existen otros protocolos de distribución cuántica de llaves. Información técnica sobre estos protocolos y otras técnicas dedicadas al ocultamiento de información usando sistemas cuánticos (por ejemplo, tecnología cuántica y su relación con Blockchain y procesamiento de imágenes) puede encontrarse en [21, 22, 23, 24, 26, 27, 28, 29, 30].

2.2 Algoritmos cuánticos

Construir computadoras sin aprovechar las propiedades físicas de los materiales usados es como escribir un relato usando pocas palabras: la capacidad de contar el cuento está limitada no sólo por la imaginación, también lo está por la pobreza del lenguaje empleado en el relato. Ampliar el vocabulario empleado abona a la mejora del cuento; de la misma forma, enriquece sumar la física de los sistemas de procesamiento de datos a los modelos matemáticos computacionales.

La computación cuántica es una disciplina dedicada al desarrollo de computadoras y programas cuyo comportamiento se describe y predice empleando las leyes de la física cuántica. El objetivo es desarrollar *hardware* y *software* para resolver problemas de altísima complejidad y gran importancia en la ciencia y la industria.

Un algoritmo cuántico es un procedimiento que usa mecánica cuántica para solucionar un problema. La creación de algoritmos cuánticos es una tarea de alto nivel científico pues, además de resolver el problema para el que fue diseñado, un algoritmo cuántico debe tener ventajas adicionales sobre cualquier algoritmo clásico pensado para solucionar el mismo problema (por ejemplo, ser más rápido).

Entre los algoritmos cuánticos más famosos se encuentra el creado por Peter Shor en 1994 [5]. La contribución de este artículo consiste en presentar un algoritmo cuántico capaz de factorizar un número entero rápidamente. La importancia del algoritmo de Shor en el contexto de la ciberseguridad deriva de lo siguiente:

En la sección 3.1, comentamos que existen dos tipos de métodos de encriptación: simétricos y asimétricos. Los asimétricos utilizan una llave pública y otra privada para hacer los procesos de ocultamiento y develación de datos.

El protocolo RSA [32], una de las implantaciones más conocidas de criptosistemas asimétricos, debe su popularidad al balance de seguridad y practicidad que observa. El protocolo RSA es empleado por gobiernos en muchos tipos de transacciones digitales. También es empleado por prácticamente todas las empresas que venden productos y servicios a través de Internet.

La seguridad de RSA radica en una conjetura matemática: la dificultad de encontrar los factores primos de un número entero. Por ejemplo, 7 y 5 son los factores primos de 35 pues 7 y 5 son números primos y 35 = 7x5. En la misma lógica, los factores primos de 485 son 5 y 97 pues 485 = 5x97 y, además, 5 y 97 son números primos. Un último ejercicio, 5336921 =127 x 42023, debe permitirnos ver que el tiempo que hay que invertir en encontrar factores primos crece conforme también crece el número entero que deseamos factorizar.

La factorización en primos de un número entero está garantizada, siempre es posible hacerla [33]. La dificultad de encontrar los factores primos de un número entero radica en que, al día de hoy, no hay un solo algoritmo que, corriendo en computadoras convencionales, pueda hacer este proceso en poco tiempo. Por ejemplo, con los algoritmos y computadoras actuales, podemos tardarnos cientos de años en encontrar los factores primos de números de mil dígitos.

De lo anterior emana la importancia del algortimo de Shor: la seguridad del protocolo RSA, consistente en los largos tiempos requeridos para factorizar números enteros muy grandes, queda seriamente lastimada con la aparición

del algoritmo de Shor pues éste es capaz de encontrar, en minutos u horas, los factores primos que a otros algoritmos tomaría siglos.

2.3 Tecnologías emergentes y su relación con la tecnología cuántica

Aprendizaje computacional cuántico. El aprendizaje computacional (*Machine Learning*, en inglés) es una rama de la ciencia computacional que, con base en técnicas estadísticas, cálculo de correlaciones y reglas emanadas del conocimiento experto en diversos dominios, desarrolla algoritmos para: a) identificar y clasificar patrones desconocidos, y b) desarrollar estrategias, basadas en la experiencia, para resolver problemas complejos.

Los sistemas de aprendizaje computacional, en boga durante los últimos años, son útiles para identificar tendencias y comportamientos anómalos en redes complejas, los mercados financieros por ejemplo. El aprendizaje computacional, sumados a otras disciplinas como la visión computacional, son la base de sistemas avanzados de vigilancia, supervisión y seguimiento (*tracking*). Ejemplo concreto de uso de aprendizaje computacional en ciberseguridad es su empleo en predicción de actividades criminales [33,34].

Los orígenes del aprendizaje automático se remontan a 1950, con los trabajos de Turing, Minsky y otros científicos [35]. A pesar de los avances cruciales en esta disciplina, un inconveniente constante del aprendizaje computacional es que la ejecución de sus algoritmos tiende a requerir mucho poder de cómputo. Esto se debe a la cantidad de datos por procesar y a la complejidad de los modelos matemáticos empleados para describir problemas y situaciones de interés.

Con frecuencia, las técnicas de aprendizaje computacional requieren construir modelos en los que estamos interesados en conocer el valor máximo de una variable. Este tipo de problemas se llaman de **optimización**. Algunos ejemplos son: ¿cuál es la demanda máxima de energía eléctrica, segmentado por horas y municipios, que se espera que consuma la ciudad de México en los siguientes seis meses? o ¿cuál cara, de todas las que están en nuestra base de

imágenes, es la más parecida al rostro de una persona grabada en un aeropuerto?

Los algoritmos de optimización tienden a consumir mucho tiempo y recursos computacionales, razón por la que hay comunidades científicas dedicadas a diseñar mejores algoritmos de optimización. Estas comunidades incluyen a especialistas en computación cuántica, debido a que los ordenadores cuánticos son buenos candidatos para resolver problemas de optimización (por ejemplo, vea [36] para una introducción a la programación de computadoras *D-Wave*).

El aprendizaje computacional cuántico es, entonces, una disciplina dedicada a crear algoritmos cuánticos cuyo objetivo es identificar y clasificar patrones desconocidos así como desarrollar estrategias, basadas en la experiencia, para resolver problemas complejos. Las aplicaciones que de este campo emanan, en particular las relacionadas con vigilancia en Internet y a través de redes digitales, de importancia en el mundo de la ciberseguridad. Para aprender más sobre aprendizaje computacional cuántico recomendamos la lectura de [36,37,38].

Redes cuánticas e Internet cuántico. Entre los elementos del portafolios de la tecnología cuántica encontramos, además de computadoras y sistemas de distribución cuántica de llaves, sensores cuánticos.

Estudios teóricos y experimentales sobre la recolección de datos muestran que es posible construir sensores cuánticos cuya sensibilidad (capacidad de recolección de datos) es mayor que la tecnología desarrollada al día de hoy. Ejemplos de este tipo de sensores son los empleados en la construcción de radares cuánticos [40,41] y mediciones ultraprecisas del campo gravitacional de la tierra [42].

La información generada por ordenadores, sistemas de distribución cuántica de llaves y sensores cuánticos requiere de un medio de transmisión que preserve la naturaleza cuántica de la información que se enviará, de ahí la pertinencia de construir redes cuánticas. Internet cuántico, neologismo cuya definición está en evolución constante, en esencia es la idea de tener una red mundial (como Internet) que permita la transmisión de información

cuántica entre sensores, computadoras y otros dispositivos. El estudio de las redes cuánticas y la posible creación de Internet cuántico es de clara importancia en los programas de ciberseguridad de México.

3. Tecnología cuántica y ciberseguridad en el plano internacional

La tecnología cuántica ha despertado el interés de varias naciones por sus avances y potencial impacto en ciberseguridad, nuevas tecnologías y desarrollo económico. En ciberseguridad, el uso del algoritmo de Shor en computadoras cuánticas robustas representa un reto futuro de proporciones mayúsculas para las transacciones digitales que empleen RSA, en tanto que la distribución cuántica de llaves es un paradigma promisorio para la construcción y fortalecimiento de protocolos criptográficos. Respecto de nuevas tecnologías, el interés surge desde la creación de nuevos materiales para computadoras cuánticas hasta el desarrollo de algoritmos cuánticos para la solución de problemas de frontera. En todo lo anterior, la inversión que hagan gobiernos y empresas permitirá crear ramas emergentes de la industria y, con ello, nuevos empleos.

En los Estados Unidos de América existe una extensa red de organizaciones académicas, empresariales y gubernamentales dedicadas a la investigación en tecnología cuántica y sus implicaciones en ciberseguridad. Más aún, desde diciembre de 2018, con la promulgación del Acta de la Iniciativa Nacional Cuántica (*National Quantum Initiative Act*) [43], el gobierno federal de ese país coordina una agenda de investigación científica y desarrollo tecnológico centrada en la ciencia de la información cuántica (*quantum information science*).

La Iniciativa Nacional Cuántica tiene por objetivo principal "asegurar el liderazgo de los EE. UU. en la ciencia de la información cuántica" (página 4 de [43]). Entre los objetivos específicos de esta iniciativa, se encuentra "promover el desarrollo de estándares internacionales para la ciencia cuántica de la información y la seguridad tecnológica" y, en particular, "alcanzar metas económicas y de seguridad nacional" de los Estados Unidos de América (página 4 de [43]). Además, la Iniciativa Nacional Cuántica tiene un subcomité en el que participan El Instituto Nacional de

Estándares y Tecnología (*NIST*, por su siglas en inglés), la Dirección de Inteligencia Nacional, el Departamento de la Defensa y la NASA. El NIST tiene por encargo convocar a un consorcio de personas y empresas interesadas en el crecimieno de la industria de la tecnología cuántica, siendo la ciberseguridad uno de los aspectos a desarrollar (página 7 de [43]) .

Desde el inicio del siglo XXI, la Unión Europea tiene un programa de amplio alcance para el desarrollo de tecnología cuántica que incluye temas prioritarios para la ciberseguridad europea, entre los que destacan [12]:

- La construcción de computadoras cuánticas robustas. Estas máquinas tendrán los sistemas de control y corrección de errores necesarios para ejecutar el algoritmo de Shor, entre otros algoritmos cuánticos.
- Generación de números aleatorios. Estos números, que son insumo crucial para diversas ramas de la ciencia y tecnología, no pueden ser generados por computadoras digitales convencionales.
- Redes de comunicaciones cuánticas de alcance continental. Estas redes constituirán la primera versión del Internet Cuántico Europeo.
- La infraestructura necesaria para hacer distribución cuántica de llaves.

Algunos de estos temas convergen, con otras tecnologías, en uno de los objetivos centrales de la ciberseguridad europea: la creación de los mecanismos y herramientas que permitan dotar, a todo habitante europeo, de identidad digital. Dado que el anonimato es un factor toral en la comisión de delitos en el ciberespacio, la creación de identidades digitales permitirá reducir significativamente el campo de acción de cibercriminales en robo de identidad, por ejemplo. Otro objetivo que comparten EE UU, Europa y países asiáticos es el desarrollo de protocolos criptográficos post-quantum, esto es, métodos de ocultamiento y develamiento de datos capaces de resistir ataques cuánticos.

4. Tecnología cuántica y ciberseguridad en México

Si bien existen algunos estudios y marcos de referencia preliminares [44,45], la construcción de la estrategia digital

mexicana es un proceso en ciernes, hecho que nos pone en desventaja respecto de agrupaciones delincuenciales dedicadas a la extorsión y robo de información por medios digitales [45]. Empero, este estado de las cosas es también una oportunidad para construir una estrategia que incluya la opinión y participación de los sectores público, académico y privado, de hacer de la estrategia un productor de conocimiento así como un detonador de desarrollo y nuevos mercados.

Uno de esos nichos con amplias oportunidades para México es la tecnología cuántica para la ciberseguridad. En este sentido, cualquier estrategia de ciberseguridad debería comprender al menos los siguientes rubros:

- Distribución cuántica de llaves.
- Redes cuánticas.
- Algoritmos cuánticos.
- Criptografía post-cuántica.
- Generadores portátiles de números aleatorios.

México cuenta con científicos e infraestructura para avanzar en los aspectos teóricos, experimentales y de implantación de la tecnología cuántica. México cuenta con capital humano e instituciones como el grupo de ciberseguridad del Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE), el laboratorio de fotónica cuántica del Centro de Investigaciones en Óptica (CIO), los Institutos de Física, Ciencias Nucleares y Matemáticas Aplicadas de la UNAM, el Centro de Investigación en Computación del IPN, CINVESTAV, el Instituto de Física de la Universidad Autónoma de San Luis Potosí y el Grupo de Procesamiento Cuántico de la Información del Tecnológico de Monterrey Campus Estado de México, entre otras organizaciones de educación superior y centros de investigación. Estas mismas instituciones serían clave en la formación del capital humano requerido para el diseño e implantación de estrategias basadas en tecnología cuántica.

En el ámbito empresarial, el ecosistema es generoso en tamaño y oportunidades. Desde desarrollos puntuales hechos por emprendedores hasta la participación de *clusters* de tecnologías de la información como los existentes en Guadalajara y Yucatán, la comunidad empresarial mexicana dedicada a la innovación tecnológica vería en

la tecnología cuántica para ciberseguridad un área de crecimiento y de protección para ella misma.

Finalmente, nuestra nación está en posibilidad de asumir el liderazgo regional en la creación de tecnología cuántica para ciberseguridad pues, en toda América Latina, solamente Brasil cuenta con capacidades similares a las nuestras en capital humano e infraestructura científico-tecnológica.

Conclusiones

La tecnología cuántica ha logrado atraer, por su desarrollo actual y prometedor potencial en la solución de problemas científicos y tecnológicos de frontera, la atención de matemáticos, físicos, científicos computacionales, ingenieros, economistas, mujeres y hombres de negocios, políticos y estudiantes, entre otros.

En tecnología cuántica, México está hoy en la encrucijada de ser agente activo en esta revolución científica y tecnológica, y así formar parte del muy selecto grupo de países que dominarán los mercados de esta tecnología, o bien quedarse en la orilla y convertirse en simple consumidor del conocimiento y aplicaciones que hoy se gestan. En particular, el desarrollo de tecnología cuántica y capital humano especializado en este rubro es de capital importancia para la ciberseguridad de nuestra nación.

BIBLIOGRAFÍA

[1] Andress, Jason. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Elsevier, MA, USA, 2014.
[2] Acín, A. et al, “The quantum technologies roadmap: a European community view”, New Journal of Physics, vol. (20), 2018, 080201.
[3] Russo, M., Thaker, A., and Adam, S. “The Coming Quantum Leap in Computing”. A Boston Consulting Group Report (2018). Recuperado el 27/marzo/2019 del sitio https://www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx

[4] "The quantum age: technological opportunities". The UK Office for Science (2018). Recuperado el 27/marzo/2019 del sitio https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf
[5] Shor, P., "Polynomial-Time Algorithms for Prime Factorization and Discrete Algorithms on a Quantum Computer", Proc. of the IEEE 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.
[6] Grover, L.K., "A fast quantum mechanical algorithm for database search", Proceedings of the 28th annual ACM symposium on the Theory of Computing, 1996, pp. 212–219.
[7] Childs, A.M., Cleve, R., Deotto, E., Farhi, E., Gutmann, S., and Spielman, D. "Exponential algorithmic speedup by quantum walk", Proceedings of the 35th ACM Symposium on The Theory of Computation (STOC'03) ACM, 2003, pp. 59–68.
[8] https://www.idquantique.com/
[9] https://www.research.ibm.com/ibm-q
[10] https://www.dwavesys.com
[11] Allende López, Marcos y Da Silva, Marcelo Madeira. Tecnologías cuánticas. Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social. Reporte técnico (white paper), Banco Interamericano de Desarrollo, 2019. DOI:10.18235/0001613
[12] Riedel, M., Kovacs, M., Zoller, P., Mlynek J., and Calarco T., "Europe's Quantum Flagship initiative" Quantum Science and Technology, vol. (4), No. 2020501, 2019.
[13] Unión Internacional deTelecomunicaciones. Recomendación UIT-T X.1205, página 3, de la serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad (abril 2008). Recuperado el 28 de marzo de 2019 de https://www.itu.int/rec/T-REC-X.1205-200804-I/es UIT–T X.1205
[14] Orús, R., Mugel, S., and Lizaso, E., "Quantum computing for finance: Overview and prospects", Reviews in Physics, vol. (4), 2019, 100028.
[15] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein–

Podolsky–Rosen Channels. Phys. Rev. Lett. 70 (13), pp. 1895–1899 (1993). DOI:10.1103/PhysRevLett.70.1895

[16] G.S. Vernam. Secret signaling system. US Patent US1310719A (1918)

[17] A. Ray Miller. the cryptographyc mathematics of Enigma. Cryptologia vol(19) No. 1, pp. 65-80 (1995). DOI: 10.1080/0161-119591883773

[18] https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/

[19] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179 (1984).

[20] Richard A. Mollin. An Introduction to Cryptography (2nd Edition). CRC Press (2006).

[21] Abd-El-Atty B., Venegas-Andraca S.E., Abd El-Latif A.A. Quantum Information Protocols for Cryptography. In: Hassanien A., Elhoseny M., Kacprzyk J. (eds) Quantum Computing: An Environment for Intelligent Large Scale Real Application. Studies in Big Data, vol 3, pp. 3--23, Springer . (2018). DOI: 10.1007/978-3-319-63639-9_1

[22] S. Loepp and W.K. Wootters. Protecting Information: From Classical Error Correction to Quantum Cryptography. Cambridge University Press (2006)

[23] Ekert, A.K., "Quantum cryptography based on Bell's theorem". Physical Review Letters vol. 67(6), 00. 661--663, 1991.

[24] Bennett, C., "Quantum cryptography using any two nonorthoganol states.", Phys. Rev. Lett. 68, 1992, pp. 3121-3124.

[25] S.E. Venegas-Andraca and J.L. Ball. Processing Images in Entangled Quantum Systems. Quantum Information Processing, vol. 9(1), pp. 1-11 (2010). DOI:10.1007/s11128-009-0123-z

[26] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca. A survey of quantum image representations. Quantum Information Processing 15(1), pp. 1-35 (2016). ISSN: 0960-1295 (print), ISSN: 1469-8072 (online). https://doi.org/10.1007/s11128-015-1195-6

[27] A.A. Abd EL-Latif, B. Abd-El-Atty, and S.E. Venegas-Andraca. A novel image steganography technique based on quantum substitution boxes. Optics and

Laser Technology 116, pp. 92-102 (Aug 2019). https://doi.org/10.1016/j.optlastec.2019.03.005

[28] C. Vlachou, Walter Krawec, Paulo Mateus, Nikola Paunkovic, Andre Souto. Quantum key distribution with quantum walks. Quantum Inf Process (2018) 17: 288. https://doi.org/10.1007/s11128-018-2055-y

[29] A.K. Fedorov, E.O. Kiktenko, and A.I. Lvovsky, "Quantum computers put blockchain security at risk", NAture vol. 465, pp. 465-467 (2018).

[30] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov, "Quantum-secured blockchain", Quantum Sci. Technol. 3, 035004 (2018).

[31] R.L. Rivest, A. Shamir, and L.M. Adleman. Cryptographic communications system and method. Patent US4405829A (filed on 14/Dec/1977, anticipated expiration on 20/Sep/2009).

[32] Gauss, Carl Friedrich; Clarke, Arthur A. Disquisitiones Arithemeticae (Second, corrected edition, translation from Latin to English). Springer (1986).

[33] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, vol. 6, pp. 35365-35381 (2018) doi: 10.1109/ACCESS.2018.2836950

[34] https://www.ted.com/talks/anne_milgram_why_smart_statistics_are_the_key_to_fighting_crime

[35] N.J. Nilson. The quest for Artificial Intelligence. Cambridge University Press (2010).

[36] Venegas-Andraca, S.E., Cruz-Santos, W., McGeoch, C., and Lanzagorta, M., "A cross-disciplinary introduction to quantum annealing-based algorithms", Contemporary Physics 59(2), 2018, pp. 174-196.

[37] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S., "Quantum machine learning", Nature 549, 2017, pp. 195-202.

[38] Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An introduction to quantum machine learning. Contemporary Physics 56(2), pp. 172-185.

[39] M. Lanzagorta, O. Jitrik, J. Uhlmann, S.E. Venegas-Andraca. Quantum Synthetic Aperture Radar. SPIE Defense + Security 2017, Anaheim, CA, EE UU. Proc. of SPIE Vol. 10188, 101880D, Radar Sensor Technology XXI (April 2017); doi: 10.1117/12.2262645.

[40] M. Lanzagorta and S.E. Venegas-Andraca. Algorithmic Analysis of Quantum Radar Cross Sections. Proc. SPIE 9461 Radar Sensor Technology XIX; and Active and Passive Signatures VI, Quantum Radar, 946112-946112-8, doi:10.1117/12.2177238 (2015).

[41] C Freier, M Hauth, V Schkolnik, B Leykauf, M Schilling,H Wziontek, H-G Scherneck, J Müller, and A Peters, "Mobile quantum gravity sensor with unprecedented stability", 8th Symposium on Frequency Standards and Metrology, Journal of Physics: Conference Series 723, 2016, 012050.

[42] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. Science vol. 362, Issue 6412, eaam9288 (2018). DOI: 10.1126/science.aam9288

[43] USA Congress. National Quantum Initiative Act. Recuperado el 31/marzo/2019 de la dirección https://www.congress.gov/bill/115th-congress/house-bill/6227

[44] Estrategia Nacional de CIberseguridad (2018). Gobierno de los Estados Unidos Mexicanos 2012-2018. Recuperado el 08/abril/2019 del sitio https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[45] Tendencias de Seguridad Cibernética en América Latina y el Caribe. Organización de los Estados Americanos (2014). Recuperado el 08/abril/2019 del sitio https://www.sites.oas.org/cyber