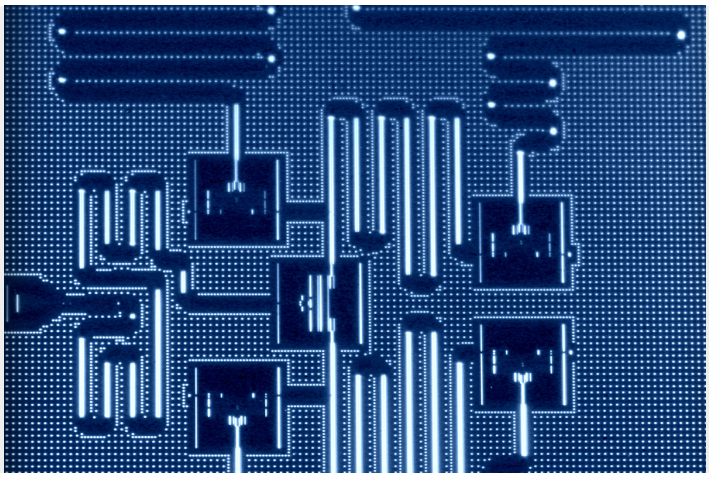
DEL CÓMPUTO CUÁNTICO Y DE SUS UNIVERSOS PARALELOS PARTE 2

Posted on 12 septiembre, 2017 by Francisco Rodríguez Henríquez



Aplicaciones comerciales que podrían ejecutarse satisfactoriamente con computadoras cuánticas que exhiban supremacía cuántica, exhiben muchas. Particularmente las industrias automotrices, así como las químicas y las genéticas están sumamente interesadas en simuladores cuánticos que les permitan emular sus procesos con una precisión y una velocidad que no estarían al alcance ni siquiera de las súper computadoras más poderosas del mundo.

Category: Ciencia

Tags: Columnas ciencia, De vértices y vórtices

Viene de Parte 1

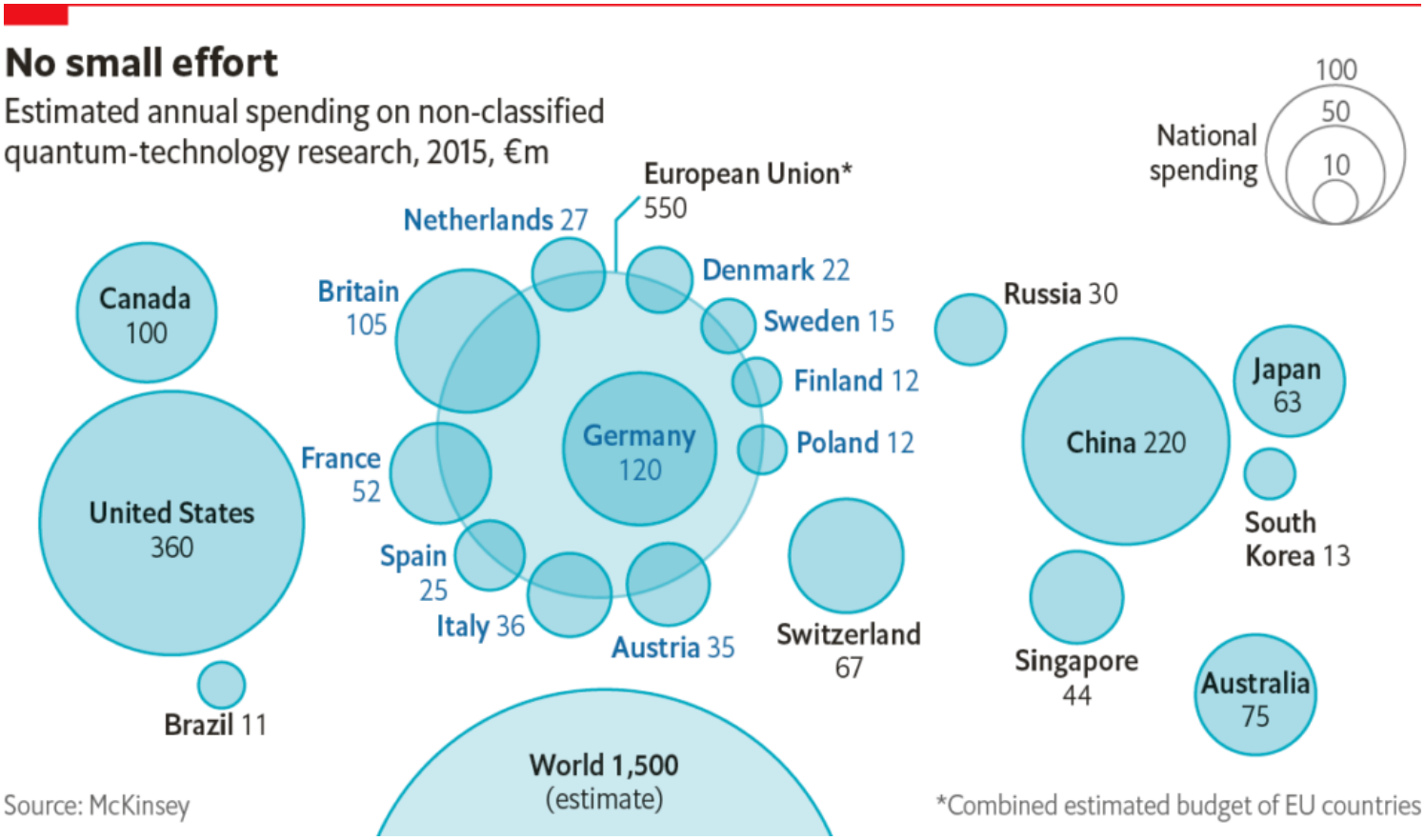


Figura 3. Inversión a nivel mundial en tecnología cuántica

Aplicaciones del cómputo cuántico en la industria

Existe un gran número de aplicaciones comerciales que podrían ejecutarse satisfactoriamente con computadoras cuánticas que exhiban supremacía cuántica. Particularmente las industrias automotrices, así como las químicas y las genéticas están sumamente interesadas en simuladores cuánticos que les permitan emular sus procesos con una precisión y una velocidad que no estarían al alcance ni siquiera de las súper computadoras más poderosas del mundo. La figura 3 muestra cómo se están invirtiendo en el mundo los fondos de investigación hacia la creación de computadoras cuánticas, en donde los Estados Unidos aparecen a la cabeza de los países que más invierten hacia la consecución de este objetivo. No obstante, recientemente la Comunidad Europea anunció un fondo especial de mil millones de euros, cuyo fin será el de obtener la supremacía a nivel mundial en la investigación y desarrollo de computadoras cuánticas para el viejo continente.

Resulta notable (y triste entre nosotros), que el único país latinoamericano que figura en el mapa de la Figura 3 sea Brasil y que México brille por su ausencia.

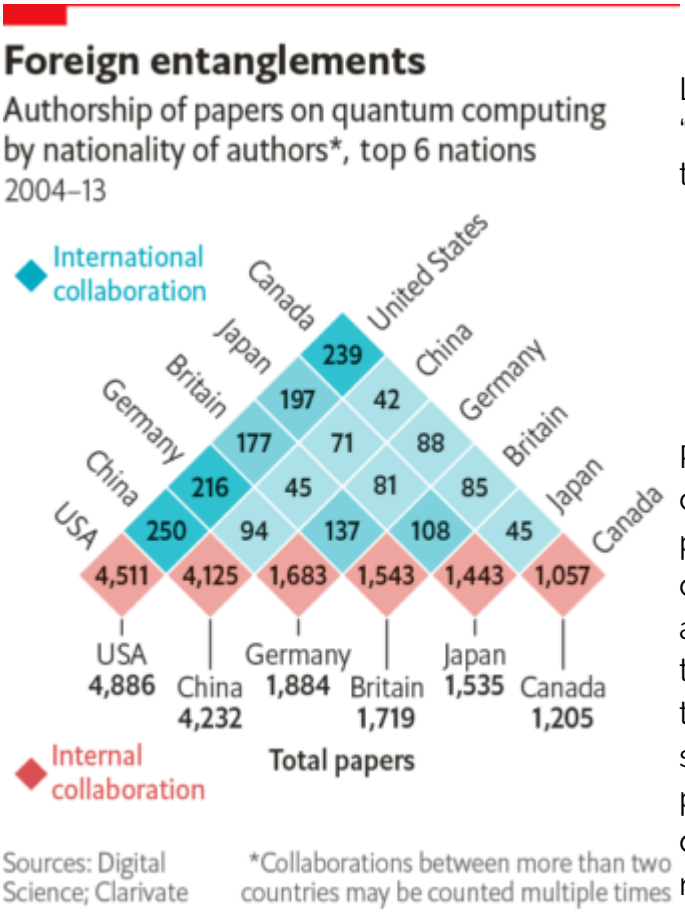


Figura 4. Colaboraciones internacionales en cómputo cuántico

La Figura 4 muestra un interesante reporte de "entrelazado científico" en la producción de artículos técnicos que tratan el tema de computación cuántica.

Aplicaciones del cómputo cuántico en la criptografía

Partiendo del supuesto de que los ordenadores cuánticos son una realidad y que están disponibles para su uso académico y comercial, científicos computacionales han propuesto una serie de algoritmos que están especialmente diseñados para tomar ventaja de las características *sui generis* que tales dispositivos electrónicos ofrecerían. Por ejemplo, se han propuesto (e implementado comercialmente), protocolos de criptografía cuántica que permiten que dos partes, digamos Alicia y Betito, se comuniquen de manera segura sin que exista la posibilidad de que un oponente, digamos Eva, sea capaz de alterar y/o espiar la comunicación de los datos que hayan sido intercambiados entre ellos, pues tal intromisión supondría la violación de principios físicos fundamentales de la mecánica cuántica. De esa manera, los protocolos criptográficos cuánticos prometen ofrecer lo que nunca lograron cumplir del todo los protocolos criptográficos clásicos, esto es, una comunicación segura y confidencial en la cual sea imposible que ningún oponente pueda modificar o discernir los datos intercambiados por las partes legítimamente involucradas en una transacción electrónica .

Aplicaciones del cómputo cuántico en criptoanálisis

Acaso más sorprendentemente, Peter Shor propuso en 1992 un celebrado algoritmo que, de ser ejecutado en una computadora cuántica poderosa, permitiría resolver el problema de factorización entera en un tiempo con complejidad polinomial al tamaño del número entero analizado. Más aún, el algoritmo de Shor puede ser fácilmente modificado para resolver eficientemente un problema más general conocido como el Problema del Subgrupo Escondido (PSE).

> *Desde el bando de los criptógrafos no todo está perdido.*

La resolución del PSE en tiempo polinomial implica que los criptosistemas de firma digital empleados en la actualidad como piedra angular del comercio electrónico, transacciones bancarias electrónicas, e-gobierno, etc., entre los que se cuentan *RSA*, DSA, ECDSA y la criptografía basada en emparejamientos bilineales, entre otros, estarían todos "rotos" pues sus garantías de seguridad basadas en la intratabilidad computacional de la factorización de enteros y del problema del logaritmo discreto, no se sostendrían más.

Sin embargo, desde el bando de los criptógrafos no todo está perdido, pues el algoritmo de Shor no permite romper todos los esquemas criptográficos clásicos existentes, y a pesar de que existen otras propuestas de procedimientos cuánticos (notablemente las que utilizan el algoritmo de Grover), que sí se pueden aplicar en algunos de los criptosistemas clásicos que sobrevivirían a los ataques al PSE, tales propuestas exhiben complejidad sub-exponencial, por lo que los criptosistemas atacados todavía se considerarían seguros. Resulta especialmente notable, por lo inesperado, que la gran mayoría de algoritmos criptográficos simétricos (también conocidos como criptosistemas de llave secreta), sean capaces de resistir todos los ataques cuánticos desarrollados hasta ahora.

En general, se define como sistemas criptográficos post-cuánticos (o resistentes a lo cuántico), a los esquemas que están fundamentados en la intratabilidad computacional de problemas computacionalmente difíciles para los cuales el algoritmo de Shor y otros procedimientos cuánticos no se pueden aplicar de manera efectiva.

Cómputo cuántico y su relación con la teoría de la complejidad computacional

Para el análisis de las bondades de un sistema cuántico resulta indispensable recurrir a la teoría de la complejidad computacional y a su clasificación de problemas computacionales en distintas clases no necesariamente disjuntas.

> *Las computadoras cuánticas únicamente ejecutan algoritmos probabilísticos.*

La clase de problemas que pueden ser resueltos eficientemente por algoritmos determinísticos y probabilísticos utilizando computadoras clásicas se conocen como P y BPP, respectivamente. En cambio, la clase NP se define como el conjunto de todos los problemas computacionales que pueden ser resueltos en tiempo no determinístico polinomial. La clase PSPACE engloba los problemas que pueden computarse con complejidad espacial polinomial. Dado que las computadoras cuánticas únicamente ejecutan algoritmos probabilísticos, la contraparte cuántica de la clase BPP se llama BQP (bounded error, quantum, polinomial time por sus siglas en inglés). Se sabe que tanto el problema de factorización entera como el del problema discreto se encuentran en BQP, pero probablemente tales problemas no están en BPP. Se sabe además que: P NP PSPACE y también que P BQP PSPACE, pero se ignora casi todo lo demás, incluyendo la que se considera la pregunta más importante de las ciencias computacionales, si acaso P = NP.

Un error bastante generalizado es el de pensar que una computadora cuántica puede resolver cualquier problema en la clase NP en tiempo polinomial. En general, no se sabe que esto sea cierto, y más bien se presume que esta suposición es probablemente falsa.

Más aún, la realidad pura y dura nos indica que la abrumadora mayoría de los algoritmos clásicos no podrán ser acelerados por un artefacto cuántico. En particular, dado que una máquina de Turing puede simular una computadora cuántica sabemos que el conjunto de problemas indecidibles para computadoras clásicas también lo son para computadoras cuánticas. Esto implica que los humanos hemos sabido idear problemas que no pueden ser resueltos por ningún modelo de computadora conocido, ya sea clásico o cuántico.

Desde el punto de vista de la criptografía post-cuántica la pregunta de si BQP NP es verdadera o falsa, es quizás la más relevante de todas. Si efectivamente la conjetura BQP NP es cierta, entonces habría que diseñar criptosistemas cuya seguridad descanse en problemas difíciles de la clase NP, conocidos como problemas NP -completos (véase Figura 5). Por el contrario, si NP BQP, entonces la única alternativa que se vislumbra es la de definir criptosistemas cuya seguridad descanse en problemas indecidibles.

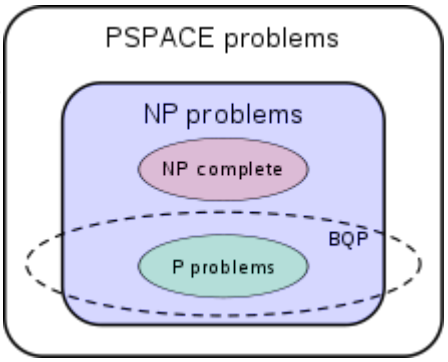


Figura 5. Clases de problemas computacionales

Resonancias filosóficas

Las razones por las cuales la naturaleza o dios, dependiendo del punto de vista del lector, “escogió”

utilizar vectores de norma-2 con coeficientes complejos para describir el comportamiento de un qubit da pie a un debate que ese esencialmente de índole filosófico . Desde el punto de vista matemático puede argumentarse que los números complejos forman la cerradura algebraica de los reales y que por lo tanto es "natural" que los coeficientes de los qubits sean números complejos (y no reales). Por otro lado, aunque pueden definirse normas más altas que la norma-2 (en la norma-3, por ejemplo, es la suma de los cubos de los componentes la que debe ser igual a 1), Scott Aaronson quien actualmente dirige el Centro de Información Cuántica de la Universidad de Texas en Austin, demostró en un artículo científico de su autoría que sólo es posible definir transformaciones unitarias no triviales que preserven la norma, en vectores definidos con norma-1 y con norma-2. Y dado que la naturaleza o dios, es muy "inteligente", entonces "decidió" escoger el mejor regalo posible para el mundo cuántico, esto es, vectores de norma-2 con coeficientes complejos.

¿Qué tal con esa línea de argumentación?

Otro debate interesante es especular de dónde salen los recursos para resolver los estados en superposición de digamos 300 qubits. Como hemos visto, esto sólo podría ser simulado con una computadora clásica con recursos de memoria superiores a 2^{300} bits, lo cual es un número muy por encima del número estimado de protones en el universo conocido . Si alguna vez una computadora cuántica de 300 qubits es construida, entonces estaríamos ante la incómoda evidencia de que la naturaleza cuenta con una matemática con "capacidades alienígenas" para resolver problemas computacionalmente difíciles que nuestro limitado y modesto conocimiento clásico consideraba intratables.

Quizás una pregunta aún más perturbadora sería la siguiente: Si algún día logramos construir una computadora cuántica universal equipada con miles de qubits, ¿habríamos demostrado la existencia de universos paralelos?

> *Aunque los universos paralelos en verdad existan, ellos deben estar dispuestos a interactuar.*

Esta pregunta surge de la observación de que la superposición cuántica implica que todos los estados en superposición de alguna manera existieron en nuestra realidad al mismo tiempo. Sin pretender analizar esta cuestión a profundidad, vale la pena observar que aun si la pregunta del párrafo de arriba pudiese contestarse afirmativamente, de todas formas, estaríamos hablando de universos paralelos que interactúan entre sí para alcanzar un resultado duradero: el estado final de los qubits cuando estos decaen al estado de decoherencia. Así, aunque los universos paralelos en verdad existan, ellos deben estar dispuestos a interactuar y coludirse para dar respuestas en nuestro prosaico, pero al mismo tiempo hermoso e ineludible mundo clásico.

Figura 6a

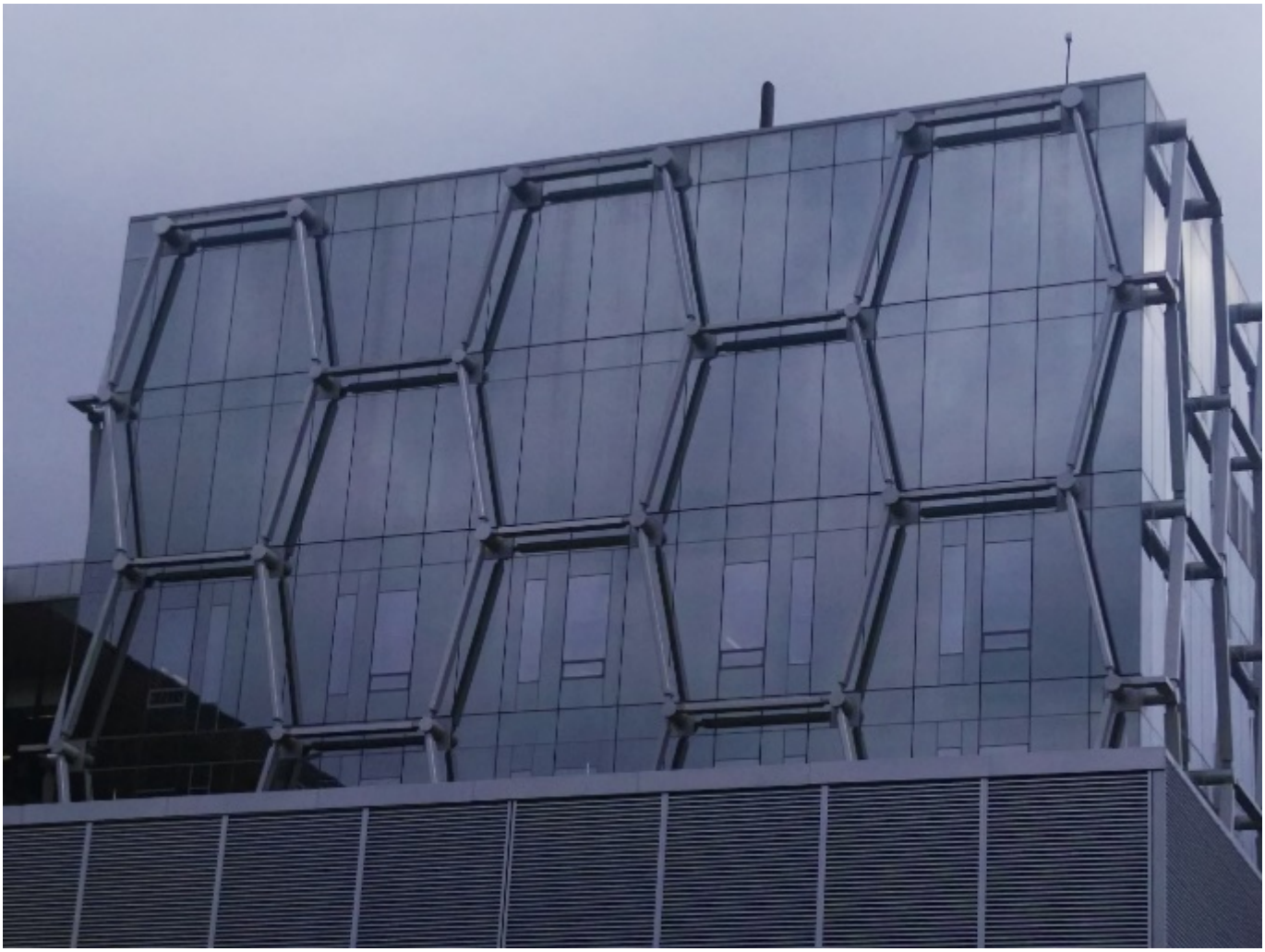


Figura 6b. Figura 6. Edificio del Institute for Quantum Computing de la Universidad de Waterloo

Figura 7a

Figura 7b. Figura 7. Gansos canadienses retozando en el campus de la Universidad de Waterloo

Conversación en el Instituto

¿Estás contento Mike? -Pregunté mientras franqueaba sin tocar la puerta entreabierta de su oficina.

Había tenido la precaución de esperar a que el locutor que narraba el partido de *soccer* que Mike veía en su computadora, un deporte que ni me interesaba ni entendía, anunciara que el partido había concluido. La oficina de Mike estaba ubicada en el quinto piso del espléndido edificio del *Institute for Quantum Computing*, no muy lejos del *Perimeter Institute*, desde donde había llegado yo caminando más lento de lo normal, rumiando mi estrategia para convencer a Mike de confiarme sus maravillosas técnicas cuánticas que por supuesto jamás se había molestado en escribir, y de la que sólo sus amigos más cercanos estábamos enterados de su existencia (aunque pensándolo mejor, no sería exagerado afirmar que por aquellos tiempos sólo yo podría ser considerado candidato a amigo

cercano de Mike). El viejo edificio donde trabajaba él estaba engalanado con los famosos ventanales diseñados para reflejar o rechazar con terca constancia los rayos solares del verano canadiense, con esa tan lograda metáfora arquitectónica que intentaba emular al estado cuántico de superposición.

Como Mike no me respondía, aproveché para asomarme por su ventana, desde la que se dominaba buena parte del campus de la Universidad de Waterloo, y desde donde se veían caminar perezosos y despreocupados, a una considerable cantidad de gansos canadienses, fielmente organizados en familias, gozosos de sentirse vivos tras resistir el largo invierno y la caprichosa primavera, y de encontrarse por fin en medio del verano del año 2030, uno de los más calurosos que se recordaban.

En vez de responderme, Mike sin voltearse del todo se limitó a sonreír, extasiado con saborear las repeticiones de las mejores jugadas del partido de *soccer* en el que increíblemente Lionel Messi se acababa de convertir en el jugador más veterano en anotar y ganar una copa del mundo, la segunda en su mágica carrera de futbolista. Como un ultra fan de ese deporte, a Mike no le cabía en el cuerpo tanta felicidad. Con un toque de astucia decidí aprovechar ese momento de debilidad para preguntarle si él pensaba que tendríamos éxito en confirmar su pronóstico de hacía ya quince años, cuando afirmó que una llave de *RSA* de 2048 bits podría ser rota con una probabilidad de 1/7 en el 2026 (lo cual no ocurrió), y con una probabilidad de 1/2 en el 2031 (lo cual estaba todavía por verse). Mike tardó en contestarme. Como viniendo de otro mundo por fin me miró de frente, con sus cabellos desordenados al estilo de Einstein, y en ese momento yo no pude evitar pensar que su cabeza era un estado cuántico en superposición y casi deseé retirar mi pregunta, o que me ignorara completamente, pues temí que en el instante mismo en que las palabras salieran de su boca esa información que sólo él en el mundo conocía se perdería para siempre, pues los innumerables qubits dentro de su privilegiado cerebro pasarían irremediablemente al estado de decoherencia.

Para mi sorpresa me contestó con una pregunta inesperada usando su inglés pausado con un cierto dejo de acento quebequense: ¿Tuviste suerte convenciendo a mis colegas físicos de que la arquitectura de la computadora debe permitir cambiar arbitrariamente tanto al parámetro x como al parámetro N del algoritmo de Shor? Su pregunta me tomó fuera de guardia, y no supe qué contestar. Me molestaba recordar las interminables discusiones con el resto de los físicos cuánticos del grupo, que tendían a creer que eran ellos los que estaban haciendo Ciencia, escrita así con C mayúscula, y que en cambio nosotros, los matemáticos y científicos de la computación adscritos al grupo, apenas estábamos aportando un detalle más de la ingeniería del magno proyecto. Yo usaba mis modestos conocimientos de la teoría de números, la reina de las matemáticas como la llamó el gran Gauss, para convencer a los físicos de que el procedimiento de Shor exigía probar con muchos parámetros candidatos x, hasta que apareciera ese número entre los números capaz de revelar uno de los dos factores primos de N. A los físicos les fastidiaba modificar parámetros, porque cada cambio costaba meses de cuidadosa reconfiguración de la arquitectura de qubits encargados de corregir los errores asociados a la ineludible decoherencia. Y meses de retraso sin publicaciones y

sin resultados, significaba agregar todavía más presión de las agencias gubernamentales y compañías tecnológicas que después de más de dos décadas de apoyos millonarios, ya hacía mucho habían agotado su paciencia. Me decidí también a ignorar su pregunta. Después de una pausa le dije. Mike como te lo he repetido tantas veces, tú eres el único físico que entiende mis algoritmos, con quien puedo conversar entre iguales. Y yo soy el único miembro del grupo que sigue creyendo en tus ideas geniales, en tu capacidad para crear magia de la nada. Para halagarlo (todavía ahora me apeno de confesarlo) agregué: es como si fueras el Messi de nuestro equipo. Sin obtener la más mínima reacción de su lado, persistí. Tú y yo sabemos que si no reducimos los qubits dedicados a la corrección cuántica de errores no podremos factorizar llaves *RSA* de 2048 bits, ni el próximo año ni en cincuenta. Es cierto que fue una sensación increíble cuando en el 2026 logramos con nuestro artefacto cuántico factorizar llaves *RSA* de 256 bits, un logro para enmarcar. Pero en mala hora, ese tozudo grupo de mis colegas franceses de Nancy, con ese nombre folclórico con el que les gusta hacerse llamar, Caramba es como se nombran ¿no?, lograron resolver *RSA* de 1024 bits utilizando técnicas clásicas, y además como para humillarnos más, anunciaron su resultado horas antes de que nosotros hiciéramos lo propio. Y por ello no pudimos anunciar la supremacía cuántica para aplicaciones criptográficas que nadie ha podido presumir hasta ahora. Y mira que ese nadie incluye a *Google*, a *Microsoft*, a *IBM*, y a tantos más que han fracasado y siguen fracasando en esta empresa. Tampoco creo que la NSA lo tenga, pues a pesar de su constante sigilo, gracias a las interminables filtraciones sabemos que su computadora cuántica no ha podido pasar de unos cuantos miles de qubits. Y eso no alcanza Mike, tú lo sabes bien, para romper una llave *RSA* de 2048 bits. Mike, por favor. Necesito que me demuestres esa técnica que sólo tú dominas, que nos permitirá disminuir el número de qubits para la corrección cuántica de errores. Es obvio que yo jamás alcanzaré tu nivel de conocimientos en mecánica cuántica, pero tengo mucha más energía que tú, mucho más talento si me permites decírtelo, para reportar nuestros revolucionarios hallazgos científicos en manuscritos escritos con ese estilo seco y aburrido que tanto les gusta a ustedes los físicos. Sólo necesito los detalles, sólo necesito que me digas, cómo proceder, cómo lograr lo que nadie ha podido hacer hasta ahora. Pese a mi entusiasmo que ahora después de tantos años veo como colegial y pueril, nuevamente Mike calló.

Volteó a ver a la ventana y después de un rato largo, habló sin prisas, con voz distante y dolorosa, como en el poema de Neruda: He descubierto que no se puede disminuir ese número, me dijo. Sus palabras sonaron como una bofetada, como una sentencia de muerte. Todo ha sido una ilusión, un espejismo, mis ecuaciones estaban mal planteadas. Ni nosotros ni nadie lo logrará nunca, agregó. Pero qué les diremos a nuestros patrocinadores le pregunté con espanto. Les diremos que busquen a la rosa de Paracelso me dijo de manera críptica. Yo no supe de qué hablaba y preferí quedarme callado. Se hizo entonces un silencio largo e incómodo que se prolongó por una eternidad que debió durar por lo menos cinco minutos. Y según recuerdo fue entonces cuando decidí retirarme sin despedirme, una decisión que todavía lamento. Creo que pensé: ¿Para qué humillar más a mi amigo con despedidas insulsas? Pero quizás sólo salí dominado por la derrota. Lo que sí supe en ese

momento fue que los días de Mike en nuestro grupo estaban contados. Y supe también como quien dice, a ciencia cierta, que sin la magia que nos prodigaba el único genio genuino de nuestro grupo, estábamos condenados a no conseguir factorizar *RSA* de 2048 bits nunca jamás. Me marché con la tristeza de quien ve pasar su última esperanza para resolver una aventura iniciada veinte años atrás que de pronto, lo supe entonces, lo sigo sabiendo ahora, se hundía sin remedio en el estado cuántico de la decoherencia. Cerré la puerta con cuidado, pero un poco antes de alejarme alcancé a escuchar apenas, sus calladas palabras de despedida: Scott, me dijo. Te urge leer los beneficios y maleficios de Jorge Luis Borges, haz tiempo para estudiarlos. Y después coloca alguna frase profunda de él que a ti te guste especialmente como epígrafe para tu próximo libro.

Al día siguiente Mike dejó el grupo sin esperar a que lo despidieran. Desde entonces no ha vuelto a escribir en ningún foro científico relevante. Y con todo este tiempo y distancia que nos separan ahora, los dos sabemos que no nos volveremos a ver nunca. Pero si un día entre los días tuviera el coraje suficiente (pero eso no podrá ocurrir nunca), cogería mi video-celular para llamarle y preguntarle qué rayos quiso decir con eso de buscar a la rosa de Paracelso, y si tuviera tiempo, también le presentaría mis apuntes en los que mis cansados análisis siguen sin encontrar error alguno en sus ecuaciones. Pero mientras tanto, siguen pasando los meses que de pronto se vuelven años, y yo sigo viendo familias de gansos canadienses ir y venir en el campus, lo mismo en el verano que en las nieves del inclemente invierno ontariano, y todavía seguimos sin conseguir nuestro objetivo: ¿Cuánto tiempo más tendrá que pasar, me pregunto, antes de que alguno de los físicos, no importa cuál, se apiade de mí y decida por fin echarme? C^2

Para aprender más

Feynman, R.: "Simulating physics with computers". International Journal of Theoretical Physics. 21 (6): 467–488 (1982)

Scott Aaronson: “Quantum Computing since Democritus”, Cambridge University Press, Abril 2013. ISBN: 9780521199568

Scott Aaraonson, personal blog. Disponible en: http://www.scottaaronson.com/blog/

“Quantum technology beginning come its own”, The Economist, disponible en: https://tinyurl.com/yddrgalr

Guillermo Morales Luna: “Computación cuántica: un esbozo de sus métodos y desarrollos”. Revista Cinvestav, Abril-Junio 2017, pp. 42—49. Disponible en: https://tinyurl.com/yb63e9e6

John Martinis, “Prospects for a Quantum Factoring Machine” Crypto 2017 Invited Talk.

Michele Mosca, “Cybersecurity in an era with quantum computers: will we be ready?”. Cryptology

ePrint Archive: Report 2015/1075. Disponible en: https://eprint.iacr.org/2015/1075

Referencias

No obstante, en un trabajo publicado recientemente en la prestigiosa revista *Nature photonics* por un equipo de científicos noruegos junto con un joven científico potosino, se logró romper un protocolo cuántico comercial. Tras iluminar un pequeño laser en el detector de Betito, los autores de este trabajo lograron deshabilitar el detector, interceptar los bits cuánticos de la llave y convertirlo a un bit clásico que coincidía con el valor que había sido enviado previamente por Alicia.

Este debate es en cierta medida análogo a la discusión de saber por qué la ley de gravitación universal de Newton o la ley de atracción eléctrica de Coulomb son proporcionales al inverso del cuadrado de la distancia entre dos objetos: ¿y por qué no son proporcionales al inverso del cubo de la distancia? alguien podría preguntarse.

Informalmente, la cerradura algebraica se define como la extensión algebraica de un campo K tal que sea algebraicamente cerrada, de tal manera que se garantice que todas las raíces de los polinomios con coeficientes en K habitan en su cerradura.

El número de Eddington estima que el número de protones en el universo observable es de 136×2^{256} protones.