Mecánica cuántica aplicada a procesado y comunicaciones: implicaciones presentes y futuras

Autor: Sánchez Jiménez, Ricardo

Directores: Fernández Gavilanes, Milagros y Fernández García, Norberto.

Contacto: ric@coit.es

Resumen:

El objetivo de este trabajo es demostrar el enorme desarrollo que han experimentado las tecnologías cuánticas en las últimas décadas, haciendo una amplia revisión de su estado actual y estimando cuál podrá ser su evolución.

Cuando los ordenadores cuánticos alcancen la supremacía cuántica, se podrán ejecutar algoritmos que disminuirán los tiempos de resolución de problemas actualmente complejos. Estos hitos no tendrían mayor trascendencia si no fuese porque se mina la confianza en la que se basan los sistemas actuales de criptografía asimétrica. Como consecuencia, se está discutiendo el estándar de una familia de sistemas criptográficos no basados en la física cuántica, pero que se espera que sean lo suficientemente complejos de resolver por ella. No existen estándares de cifrado cuántico, pero se estudia la aplicación de sistemas de comunicaciones cuánticas en protocolos que permiten establecer con máxima seguridad un secreto compartido. Estas comunicaciones, encuentran también un nicho de oportunidad en el desarrollo de generadores cuánticos de números aleatorios, aumentando la entropía de los generadores actuales. Relacionado con el avance de la computación y de los algoritmos cuánticos, se estudia su impacto en los métodos de aprendizaje automático, con un potencial a considerar en su uso en aplicaciones de seguridad, como los sistemas de detección de intrusiones en red.

En definitiva, la definición de casos de uso basados en las diferentes tecnologías cuánticas será el detonante para su desarrollo a nivel académico, al aumentar los presupuestos de investigación. También es esperable un crecimiento de la inversión privada, dadas las múltiples aplicaciones de estas tecnologías.

Palabras clave: Cúbit, estados cuánticos, criptografía PQ, QKD, QML.

---

1. Introducción

1.1. Contexto histórico

En el primer cuarto del siglo XX se asentaron las bases de la nueva física cuántica, aconteciendo lo que se ha conocido como la primera revolución cuántica, en la que se obtiene la capacidad para acceder a estados cuánticos discretos en los sistemas. Se comienza a hablar de la "cuantización" y del efecto túnel, con el desarrollo a partir de la mitad del siglo XX, de tecnologías que se basan en el carácter discreto de la naturaleza. Encontramos ejemplos como el del diseño del primer transistor, el primer láser o las células fotovoltaicas.

Posteriormente, a partir de los años 80 llegamos a la segunda revolución cuántica, que podemos considerar que pervive hasta hoy. Se dispone de la capacidad de preparar y controlar los estados cuánticos a voluntad, gracias a propiedades como la superposición y el entrelazamiento cuántico. De esta forma, durante la última década se ha desarrollado enormemente la investigación en las tecnologías cuánticas que son objeto de este trabajo, principalmente la computación y las comunicaciones cuánticas, dado que el resto de disciplinas podemos considerarlas como una consecuencia de los avances de estas dos primeras.

1.2. Objetivos

A lo largo del presente documento se pretende transmitir al lector la relevancia del extenso concepto de las tecnologías cuánticas, poniendo de manifiesto el gran potencial que tienen desde el punto vista técnico y estratégico, obteniendo unas capacidades y unos niveles de seguridad muy superiores a los obtenidos por los métodos tradicionales.

Para conseguirlo, se hará un estudio pormenorizado de la situación actual de los ordenadores cuánticos, que van a ser del detonante del desarrollo de las otras tecnologías cuánticas, ya sea de forma directa o indirecta. Esto aplica especialmente al caso de la criptografía postcuántica (PQ) o del aprendizaje automático cuántico (QML). Podemos considerar que en el caso de las comunicaciones cuánticas y de los generadores cuánticos de números aleatorios (QRNG), están evolucionando de forma (más) independiente, pero siempre en base a las propiedades cuánticas de los elementos que manipulan, generalmente fotones de luz.

2. Motivaciones y necesidades para su desarrollo

Desde principios del siglo pasado, la física cuántica ha venido estudiando el comportamiento de las partículas de tamaño atómico, intentando explicar su comportamiento con fenómenos difícilmente explicables desde el punto de vista de la física clásica. Sin embargo, ha sido en los últimos 20 años cuando han convergido los estudios teóricos conocidos hasta la fecha, con un enorme desarrollo técnico en la implementación de los ordenadores cuánticos, que ha permitido ir demostrando uno a uno todos los postulados definidos por los físicos teóricos durante el siglo XX. Al ir pasando los estudios paulatinamente del plano teórico al escenario real, se ha vuelto a despertar el interés no sólo de la comunidad científica y la sociedad en general, sino de diferentes consorcios empresariales y agencias gubernamentales dado el enorme potencial que ofrece esta tecnología. Han entrado en el campo de juego múltiples jugadores no tradicionales, dadas las derivadas geopolíticas entre los países del bloque occidental y China, principalmente. Gartner [1] prevé que, en 2023, un 20% de las organizaciones contemplarán en su presupuesto partidas para proyectos de computación cuántica, frente al 1% de las organizaciones que lo presupuestaron en 2019.

Según la consultora de negocios BCG [2], puede haber 3 causas que expliquen el vertiginoso aumento de inversión, que va ligado a la actual carrera de investigación y desarrollo en el campo de las tecnologías cuánticas:

- Alcanzar la ansiada supremacía cuántica, ya anunciada un par de veces de manera un tanto controvertida tanto por Google [3] como por un grupo de investigación de la Universidad de Ciencia y Tecnología de China en Hefei [4]).
- Disponer de una hoja de ruta que fije hitos rupturistas a diez años vista.
- Definir casos de uso que hagan despertar el interés comercial de la industria.

3. Tecnologías cuánticas

3.1. Ordenadores cuánticos

Comenzamos haciendo referencia al concepto de supremacía cuántica, comentado al final del apartado anterior. Esta idea fue presentada por Preskill en 2012 [5]. Según su artículo, la supremacía se alcanzará cuando seamos capaces de realizar tareas con sistemas cuánticos controlados, de una complejidad mayor que las tareas más complejas que se pueden conseguir con ordenadores digitales clásicos. En el caso de Google, en 2019 [3] anunciaron que habían alcanzado la supremacía cuántica después haber superado un reto muy complejo para los ordenadores actuales. Lo consiguieron con un ordenador cuántico de 53 cúbits[1], denominado Sycamore. Desde el punto de vista de IBM [6], este reto se podía haber completado en un par de días mediante su propio superordenador clásico Summit, poniendo en discusión la autoproclamada supremacía cuántica y rebajándola a tan solo una "ventaja" cuántica.

Posteriormente, Preskill presentó un concepto en 2018 [7], utilizado para describir el punto de situación en el desarrollo de los actuales ordenadores cuánticos, en la vertiginosa carrera de investigación existente. Son los llamados ordenadores NISQ (*noisy intermediate scale quantum*). Vienen caracterizados por su gran sensibilidad respecto del ambiente que los rodea (*noisy*), lo que perturba el estado de sus cúbits. Su número de cúbits (en un orden de entre 50 y unos pocos cientos) sigue en pleno crecimiento, pero lejos de representar un valor diferenciador (*intermediate scale*). Aun así, proporciona una pequeña ventaja cuántica de procesamiento respecto de los ordenadores actuales (*quantum*).

En la Figura 1 podemos ver las diferentes apuestas que lideran varias corporaciones TIC. Destacamos los ordenadores cuánticos basados en bucles de superconductores, apuesta tecnológica de IBM, Google y Amazon. Consiguen los mejores resultados basándose en la superposición de corrientes que discurren simultáneamente alrededor de un conductor. El coste de fabricación es bajo, pero requieren de un gran esfuerzo en mantener temperaturas extremadamente bajas, para extraer la entropía introducida por el ruido [5]. Otra dificultad es el valor tan bajo del tiempo de coherencia que consiguen, del orden de milisegundos.

Sin embargo, se va consolidando la idea de un escenario híbrido altamente eficiente, en el que los ordenadores actuales pueden complementar el papel de los simuladores cuánticos. Preskill [7] hace mucho hincapié en no perder de vista el esfuerzo de I+D de puertas cuánticas con una menor tasa de

[1] El cúbit o bit cuántico, es la unidad elemental de información cuántica, equiparable en cierta forma al bit de la lógica binaria, pero de naturaleza probabilística.

error que, junto con el diseño de algoritmos cuánticos resilientes al ruido ambiente, nos permitan construir sistemas de mayor volumen cuántico. Por tanto, la motivación principal que debe marcar la investigación en la búsqueda de un ordenador cuántico debe ser obtener un sistema perfectamente aislado del mundo exterior, medible y gestionado [5].

		Superconductors	Ion traps	Photonics	Quantum dots	Cold atoms
% of potential users who consider technology "promising"		61%	35%	34%	26%	16%
Qubit quality[1]	*Qubit lifetime*	~1 ms	~50+ s	N/A	~1-10 s	~1 s
	Gate fidelity	~99.6%	~99.9%	~99.9%	~99%	~99%
	Gate operation time	~10-50 ns	~1-50 µs	~1 ns	~1-10 ns	~100 ns
Connectivity		Nearest neighbors	All-to-all	All-to-all[2]	Nearest neighbors	Near neighbors
Strengths		✓ Engineering maturity ✓ Scalability[3]	✓ Stability ✓ Gate fidelity ✓ Connectivity	✓ Horizontal scalability ✓ Established semiconductor tech	✓ Stability ✓ Established semiconductor tech	✓ Horizontal scalability ✓ Connectivity
Challenges		× Near absolute zero temperatures × Connectivity limitation in 2D	× Gate operation times × Horizontal scaling beyond one trap	× Noise from photon loss	× Requires cryogenics × Nascent engineering	× Gate fidelity × Gate operation time
Example players		IBM, Google	Honeywell, IonQ	PsiQuantum, Xanadu	Intel, SQC	ColdQuanta, Pasqal

Figura 1- Tabla resumen de las tecnologías usadas en los ordenadores cuánticos [2]

3.2. Distribución cuántica de claves

Si bien todavía no existe ningún estándar de cifrado propiamente cuántico, sí que existe un escenario de comunicaciones cuánticas basado en el transporte de fotones de luz. Empleando protocolos de distribución cuántica de claves, se puede establecer con seguridad una clave de cifrado compartida entre emisor y receptor en un canal no seguro. Se abre un campo enorme de investigación en el que se intenta reutilizar infraestructuras de comunicaciones de fibra óptica, o bien desplegar sistemas de comunicaciones ópticas en el espacio libre con línea de visión directa.

Los diferentes métodos desarrollados se han basado en transmitir fotones manipulados en función de la información codificada a transmitir. Esa manipulación ha consistido tradicionalmente bien en una polarización del fotón (en dos o cuatro bases no ortogonales, que entenderemos como orientaciones diferentes), o bien en el entrelazamiento de una pareja de fotones. Lo que se implica establecer una clasificación muy relevante, que se plasmará en los diferentes protocolos propuestos. En el caso del protocolo desarrollado en 1984 por Bennett y Brassard (BB84) [8], hace uso de fotones polarizados por el emisor y receptor, mientras que el protocolo desarrollado por Ekert en 1991 (E91) [9], hace uso de fotones entrelazados que se encuentran correlados de forma complementaria (anticorrelados, en los que al realizar una medida colapsa su estado y adquieren valores contrarios).

De forma similar a como se ha diferenciado tradicionalmente el mundo analógico del mundo digital, en la comunicación cuántica se puede distinguir el uso de valores continuos o valores discretos. Los primeros protocolos de QKD se basaron en la transmisión de señales discretas, normalmente en forma de pulsos de luz. Estos métodos son conocidos como DV-QKD, más sencillos de implementar y con un mayor alcance, acompañados de una mejor tolerancia a fallos. En el otro extremo están los

métodos basados en el envío de señales continuas (CV-QKD), propuestos por Ralph en 1999 [10]. Transmiten con una polarización fija, son más complejos, pero tienen la gran ventaja de poder compartir el canal de comunicación con otras señales existentes, lo que evita disponer de canales de comunicaciones dedicados en exclusiva para su funcionamiento. Esto favorecerá su despliegue, así como su integración en redes de comunicaciones ópticas existentes multiplexadas, como una señal más.

3.3. Criptografía postcuántica (PQ)

El desarrollo e implementación de equipos que permitan ejecutar algoritmos, que puedan representar un riesgo para la mayoría de los sistemas de cifrado actuales, es cada vez más cercano. Podemos estimar un periodo incierto de 15 años hasta el momento más crítico en el que se rompan los sistemas de cifrado vulnerables. Debido a esto, se requiere iniciar urgentemente un periodo de investigación y desarrollo, que evite la continua exposición de secretos cifrados con los algoritmos actuales. Apremia comenzar a migrar toda la infraestructura de los sistemas de cifra vigentes a nuevos estándares resistentes a dichos ataques. Estos futuros estándares son conocidos por el nombre de sistemas criptográficos post cuánticos (PQ).

En el caso de los sistemas de cifrado en bloque, que emplean claves de cifra simétrica como por ejemplo en el AES, gracias al algoritmo de Grover [11] es posible encontrar un resultado en una lista desordenada de N elementos (en este caso claves), reduciendo su complejidad (computacional) al caso en el que la lista tuviese la raíz cuadrada de N elementos. A efectos prácticos, la seguridad se reduciría de manera equivalente, al hecho de realizar un ataque clásico por fuerza bruta con una clave de la mitad de bits. Por lo que se recomienda seguir usando una longitud de clave de 256 bits, pero con la vista puesta en el avance de los ataques.

Por otro lado, la aplicación [12] del algoritmo de Simon [13] en ataques basados en la búsqueda de colisiones, posibilita acelerar su cómputo de manera exponencial. Esto permite romper diversos algoritmos de cifra simétricos empleados en autenticación y cifrado autenticado, tales como: CBC-MAC, PMAC, GMAC, GCM, y OCB, algoritmos que se pueden considerar completamente rotos.

En el caso de los sistemas de cifrado de clave pública, esta situación es considerablemente más preocupante según la aplicación del algoritmo de Shor [14], dando por neutralizada la complejidad computacional de la solución al problema de logaritmo discreto y de la factorización de números primos grandes. Ambos constituyen la base de los sistemas de cifra de clave pública, como es el caso de los sistemas de curvas elípticas (EC) y RSA.

La comunidad criptográfica lleva años estudiando la aplicación de sistemas alternativos de cifrado y firma digital, que no se basen en los problemas comentados y que eviten ser rotos por los futuros ordenadores cuánticos, al menos con el conocimiento matemático del que se dispone hoy en día. Se están estudiando algoritmos basados en:

- Retículos
- Teoría de códigos
- Isogenias
- Resúmenes
- Ecuaciones multivariables.

Ante la problemática existente, el Instituto Nacional de Estandarización y Tecnología americano (NIST), publicó un concurso en el año 2016 para buscar algoritmos alternativos a sus estándares de firma digital [15] y de establecimiento de claves [16][17], que sean resistentes a futuros ataques producidos con ordenadores cuánticos. Se pretende que los esquemas ganadores puedan modificar los protocolos potencialmente afectados (IKE, TLS, DH, IPSec, DNSSEC, etc.), para completar una transición a los nuevos algoritmos en un plazo de 10 años.

3.4. Generadores cuánticos de números aleatorios (QRNG)

Los QRNG [18] son capaces de generar secuencias aleatorias con un alto nivel de entropía, aprovechándose de las propiedades de la física cuántica, que proporcionan unas condiciones de aleatoriedad perfectas para este fin. El mero hecho de medir el estado de un sistema cuántico provoca que colapse de forma única, aleatoria e impredecible, de acuerdo con el teorema de no clonación. A esto se añade el hecho de que el sistema, tras realizar la medición, continuará evolucionando de forma probabilística.

Idealmente se basarán en soluciones hardware, pero pueden verse reforzados por complementos software, p.ej. para aumentar la tasa de generación de la secuencia de salida hasta valores del orden de Gigabits/s. En caso contrario, dado que normalmente usarán dispositivos de medida como detectores de fotones, el resultado vendrá condicionado por la capacidad de medida del detector, limitando su rendimiento al orden de los Megabits/s.

3.5. Aprendizaje automático cuántico (QML)

Los algoritmos de aprendizaje automático tradicionalmente procesan grandes cantidades de información para tareas en las que se interpretan datos. Generalmente hay dos tipos de aproximaciones de algoritmos de ML al ámbito de QML [19]:

- Desarrollo de nuevas versiones de algoritmos (cuánticos) que puedan sustituir a antiguos algoritmos (clásicos) para solucionar un problema, p.ej. en los casos de búsqueda de los k-vecinos más cercanos (k-*nearest neighbour*), agrupación de datos (*data clustering*) o reconocimiento de patrones (*pattern recognition*), donde el pesado cálculo de distancias puede ser acelerado en un ordenador cuántico.
- Utilizar la descripción probabilística de la física cuántica para traducir aquellos procesos estocásticos, como la teoría de decisión bayesiana o los modelos ocultos de Markov, a los nuevos lenguajes de programación.

Adicionalmente, hay otros modelos de ML como el caso de las redes neuronales o los árboles de decisión, que todavía siguen esperando una versión cuántica eficiente. Se pueden considerar prometedores los algoritmos cuánticos que han demostrado ser muy eficientes, como HHL o QPCA, en su aplicación para métodos de reconocimiento de patrones.

Tradicionalmente se han empleado técnicas de ML para aplicaciones de detección de intrusiones en red, conocidas como NIDS (*network intrusión detection system*), dado que se puede plantear la detección de una anomalía como un problema de clasificación para detectar un comportamiento anómalo entre otros correctos. Se puede extender la aplicación de métodos QSVM (*quantum support vector machines*) para este propósito [20].

4. Conclusiones

A lo largo del presente trabajo se ha intentado transmitir al lector una idea lo suficientemente amplia sobre el mecanismo de las diferentes tecnologías cuánticas, su capacidad, y cuál será probablemente su hoja de ruta en función de los avances que vayan obteniendo sus investigadores.

En el caso de los ordenadores cuánticos, se ha destacado el concepto presentado por Preskill acerca de los ordenadores NISQ que, aunque siguen presentando problemas de ruido y no ofrecen una gran capacidad, ofrecen una funcionalidad suficiente para que otras disciplinas puedan seguir evolucionando. Existen diferentes arquitecturas de aproximación al ordenador cuántico, con diferente grado de evolución. Podemos destacar como muy prometedora la apuesta "topológica" liderada por Microsoft, pero siendo realistas, las referencias que más están destacando incluyen diseños basados en bucles de superconductores.

Para hacer realidad una de las grandes promesas cuánticas, como ejecutar el algoritmo de Shor, siguen existiendo trabas técnicas que imposibilitan en la actualidad implementar sistemas con suficientes cúbits tolerantes a errores. Sin embargo, son muy relevantes las advertencias que hace Michele Mosca [21] cuestionando si nuestros sistemas estarán preparados a tiempo para cuando llegue ese momento.

La distribución cuántica de claves, independiente del aumento de capacidad de computación, es una tecnología a tener muy en cuenta, y prueba de ello son las inversiones multimillonarias y los grandes avances que están consiguiendo los centros de investigación chinos. Sin ninguna duda, uno de los grandes retos de QKD va a ser su integración en escenarios SDN, conjugado con ofrecer un servicio de distribución de claves como servicio (KaaS). Para que esto se puede llevar a cabo, se considera casi imprescindible el desarrollo de un sistema basado en valores continuos (CV-QKD), con el que se asegure una compatibilidad y una convivencia con los actuales medios de transmisión de fibra óptica.

En cuanto a los sistemas cuánticos de aprendizaje automático, tras revisar la literatura existente se puede considerar que, de todas las tecnologías cuánticas, esta es la que se encuentra en un estado más inmaduro, pero no implica que no se esté investigando ampliamente sobre la adaptación de sus múltiples variantes al ámbito cuántico. Hay que destacar el anuncio hecho por IBM [22] en el que declaraba haber obtenido una ventaja polinómica de cómputo en los métodos QSVM.

En definitiva, las conclusiones a las que hemos llegado y los retos planteados, vendrán muy influenciados por la inversión en I+D que se dedique en estos campos. Actualmente nos encontramos en un periodo dorado gracias a la promesa de alcanzar un hito rupturista que, con el aliciente de anuncios como los ya comentados de alcanzar la supremacía cuántica, permiten ir definiendo en mayor medida casos de uso para la industria. Lo que afortunadamente nos devuelve a la casilla de salida, incentivando la inversión privada y, en algunos casos, hasta la inversión pública.

Referencias

1. Gartner.com: The CIO's Guide to Quantum Computing [Internet]. [09 Ene **2022**]. https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing.
2. Boston Consulting Group: What Happens When 'If' Turns to 'When' in Quantum Computing? [Internet]. [09 Ene **2022**]. https://www.bcg.com/publications/2021/building-quantum-advantage?linkId=124924149.

3. Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*. **2019**; 574: 505-511.
4. Yulin Wu et al. Strong Quantum Computational Advantage Using a Superconducting Quantum *Processor Phys. Rev. Lett*. **2021**; 127, 180501.
5. Preskill J. Quantum computing and the entanglement frontier. *arXiv*. **2012**; 1203.5813.
6. IBM.com: On "Quantum Supremacy". [Internet]. **2019**. [10 Ene 2022]. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/
7. Preskill J. Quantum Computing in the NISQ era and beyond. *Quantum*. **2018**; 2: 79.
8. Bennett CH., Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. **2014**; 560: 7–11.
9. Ekert A. Quantum Cryptography Based on Bell's Theorem. Phsysical review letters. 1991; 67 (6): 661-663.
10. Ralph TC. Continuous Variable Quantum Cryptography. *arXiv quant-ph*. **1999**; 9907073.
11. Grover L. A fast quantum mechanical algorithm for database search. Proceedings, *STOC*. 1996; 212-219.
12. Kaplan et al. Breaking Symmetric Cryptosystems using Quantum Period Finding. *arXiv*. **2016**; 1602.05973: 1-31.
13. Simon D. On the power of quantum computation. *SIAM journal on computing*. **1997**; 26(5): 1474–1483.
14. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*. **1997**; 26(5): 1484-1509.
15. NIST. Digital Signature Standard (DSS). *FIPS*. **2013**; 186-4: 1-130.
16. Barker et al. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Digital Signature Standard (DSS). *NIST-SP*. **2018**; 800-56A: 1-139.
17. Barker et al. Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. *NIST-SP*. **2019**; 800-56B: 1-131.
18. Jacak M. Quantum generators of random numbers. *Nature Scientific Reports*. **2021**; 11(16108): 1-21.
19. Schuld et al. An introduction to quantum machine learning. *arXiv*. **2014**; 1409.3097: 1-19.
20. Gouveia A., Correia M. Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection. *IEEE 19th International Symposium on Network Computing and Applications (NCA)*. **2020**; 1-8.
21. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*. **2018**; 16 (5): 38-41.
22. Liu et al. A rigorous and robust quantum speed-up in supervised machine learning. *arXiv*. **2020**; 2010.02174: 1-27.