Tecnologías cuánticas de interés en defensa

Autor: Pablo Martínez Mena, Programas de Plataformas Terrestres, INDRA

Palabras clave: *qubit*, entrelazamiento, coherencia, fotón, cuántica, disruptivo.

Objetivo tecnológico: Seguimiento de tecnologías emergentes con aplicación futura a defensa.

Introducción

En las últimas décadas se viene gestando lo que se ha denominado *segunda revolución cuántica*[1]. Si en los primeros años del s. XX la comprensión de las leyes que gobiernan el mundo a escala nanométrica[2] no solo cambió nuestra visión de la naturaleza sino que alumbró productos como el láser o el transistor, los progresos recientes en el control de dicho mundo permiten explotar nuevos fenómenos que auguran hitos análogos a la microelectrónica o Internet. El ordenador cuántico persigue superar al ordenador clásico en la velocidad de procesamiento de determinados cálculos gracias al fenómeno de *superposición*[3].

Por otro lado, el fenómeno de entrelazamiento (*entanglement*) conecta entre sí partículas cuánticas de forma que los cambios en una de ellas afectan instantáneamente a su compañera, no importa a qué distancia se encuentre, sugieriendo la posibilidad de un Internet cuántico. Si bien la mayoría de estos nuevos desarrollos, agrupados bajo el término *tecnologías cuánticas,* aún se encuentran en niveles bajos de madurez tecnológica, algunas aplicaciones específicas empiezan a introducirse en el mercado. Las altas sumas económicas

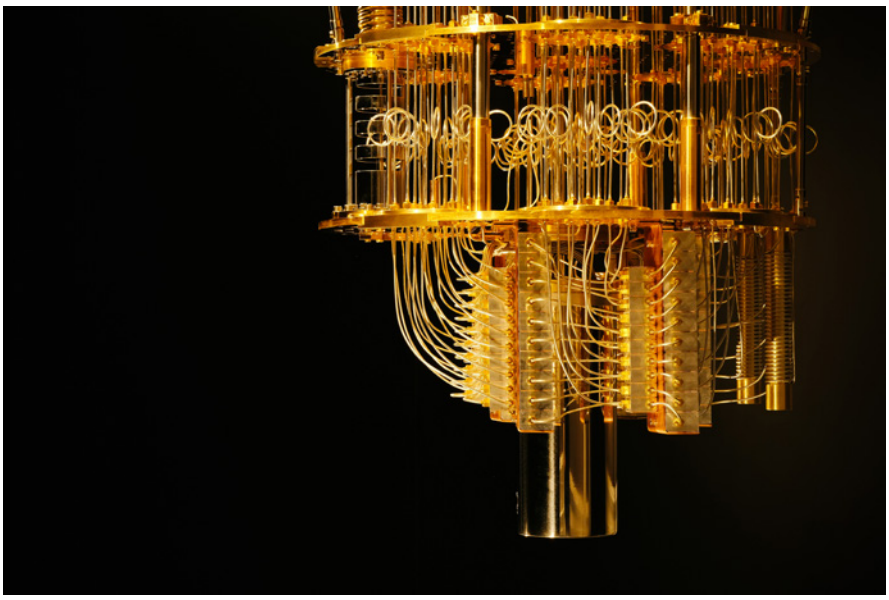

Fig. 1. Ordenador cuántico de IBM. (Fuente: IBM).

que se están invirtiendo en este campo, tanto desde el sector privado como del público, hacen merecedora a esta tendencia de un análisis en cuanto a su aplicación en el sector de la defensa, donde también despierta interés. Las tecnologías cuánticas son un conjunto heterogéneo de equipos y técnicas aplicables a muy distintos casos de uso en dicho sector; en este artículo presentaremos una clasificación de estas tecnologías y analizaremos las aplicaciones de cada categoría más prometedoras para el sector de defensa.

Clasificación de las tecnologías cuánticas y su interés en defensa

Las tecnologías cuánticas suelen clasificarse en cuatro grandes áreas, en función de su aplicación: sensores cuánticos y metrología, comunicaciones cuánticas, computación cuántica y simulación cuántica.

El área de sensores cuánticos y metrología abarca distintos dispositivos y técnicas para medir magnitudes físicas como la radiación electromagnética (imagen o iluminación cuántica), aceleraciones (sensores inerciales basados en interferometría de átomos), campos magnéticos (sensores magnéticos basados en centros nitrógeno-vacante en diamante) o el tiempo (relojes atómicos) [1]. En general, estos sensores hacen uso de los fenómenos y tecnologías cuánticas para superar la precisión o la sensibilidad de sus contrapartidas convencionales o clásicas. Esta mejora en el desempeño del sensor es la que puede ser aplicada en defensa con el fin de detectar amenazas o disponer de información más precisa sobre el entorno (mejora de la conciencia situacional).

Las comunicaciones cuánticas comprenden las aplicaciones para transmitir información o garantizar la seguridad de la misma, siendo ambas aplicaciones claves en defensa. El ámbito de la criptografía cuántica ha avanzado con rapidez debido a la amenaza que supone la capacidad de proceso del ordenador cuántico para la seguridad de los sistemas actuales de cifrado. Esto ha motivado una carrera por encontrar nuevos métodos de securización de la información, entre los que destaca la distribución cuántica de claves (*Quantum Key Distribution* o *QKD*) [2] y la criptografía poscuántica[4].

El ordenador cuántico supondría un salto de gigante respecto a la capacidad de cálculo de los ordenadores

[1] El término *cuántico* hace referencia a los paquetes mínimos (*quanta*) mediante los que se transfiere la energía a escala atómica. Este descubrimiento de Max Planck en 1900 marcó el inicio de la primera revolución cuántica.

[2] Un nanómetro es la milmillonésima parte de un metro, magnitud próxima al tamaño de los átomos.

[3] Fenómeno por el que los *bits* cuánticos o *qubits* pueden encontrarse en distintos estados a la vez.

[4] La criptografía poscuántica no es estrictamente una tecnología cuántica; su objetivo es buscar operaciones que no puedan ser eficientemente ejecutadas en un ordenador cuántico para utilizarlas en nuevos protocolos de criptografía.

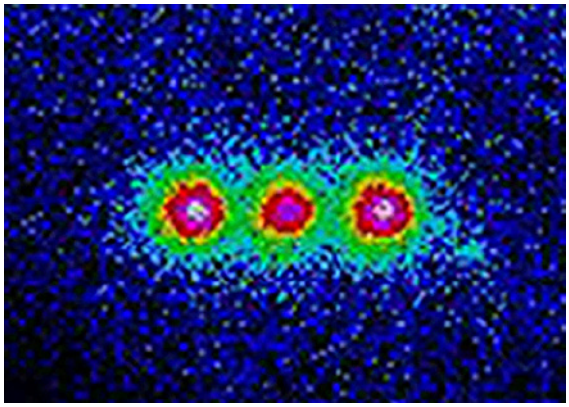

Fig. 2. Tres iones de berilio atrapados. (Fuente: NIST).

actuales [3]. Las primeras propuestas de implementaciones físicas del ordenador cuántico[5], junto con el desarrollo de algoritmos que permitirían realizar operaciones de forma más rápida que los ordenadores actuales, desataron la carrera por obtener un ordenador cuántico con aplicaciones reales. En la actualidad, hay varias implementaciones de un ordenador cuántico basadas en distintos métodos: trampas de átomos gaseosos ultrafríos, circuitos superconductores, etc. que aún han de superar arduos retos técnicos.

Por último, el área de simulación cuántica pretende comprender el funcionamiento de sistemas complejos mediante el análisis de sistemas cuánticos modelo [4]. Este área es de sumo interés en ciencia básica, pues podría ayudar al progreso en la caracterización de materiales o moléculas. En la industria de defensa, los avances en el área de simulación cuántica podrían aplicarse indirectamente mediante la obtención de nuevos materiales (más ligeros o resistentes), nuevos fármacos (antídotos para agentes de guerra química), etc.

Aplicaciones de sensores cuánticos y metrología

Imagen cuántica y radar cuántico. Las técnicas de imagen cuántica explotan el carácter corpuscular de la luz (es decir, su constitución por partículas llamadas fotones) y el alto control que se ha obtenido sobre los mismos para iluminar los objetos con haces de luz de características especiales que permiten superar los límites a la resolución que encuentran las técnicas convencionales [5]. Por ejemplo, la disponibilidad de fuentes de fotones individuales, generados a intervalos de tiempo determinados, permite obtener relaciones señal-ruido inferiores al ruido de disparo (*shot noise*) causado por las fluctuaciones en el flujo de fotones y que constituía un umbral mínimo en los detectores de luz y en los sistemas de comunicaciones ópticas.

Otra barrera bien conocida en óptica clásica es el límite de Rayleigh: el comportamiento ondulatorio de la luz convierte fuentes luminosas puntuales en una serie de discos concéntricos e impide distinguir entre sí puntos cuya separación angular sea menor que un valor determinado por la relación entre longitud de onda y la apertura con que se observa. Este límite también ha sido superado gracias al uso de estados cuánticos especiales de la luz en aplicaciones de microscopía o astronomía, aunque se espera que estas técnicas se utilicen también en la mejora de otros equipos ópticos como cámaras visibles o térmicas.

Una técnica que revela las extrañas leyes que gobiernan el mundo cuántico es la denominada *ghost imaging*. En esta técnica se explota la correlación o el entrelazamiento (*entanglement*) entre dos haces de fotones. El entrelazamiento es un fenómeno cuántico que consiste en el vínculo que se establece entre dos partículas (en este caso fotones) en el momento de su generación y que nos permite identificar uno de ellos mediante su compañero. En el *ghost imaging* se envía un primer haz de fotones al blanco, recibiendo en un detector sin resolución espacial (solo tiene un píxel) aquellos que se reflejen en el mismo (es decir, solo detecta si un fotón ha dado en el blanco, pero no en qué lugar del mismo). Simultáneamente, se envía el haz de fotones entrelazados con el primero hacia un segundo detector, este sí con resolución espacial, en el que, al combinarlo con la señal del primer detector, se forma la imagen del blanco. Lo notable es que la imagen la forma el haz que no ha interactuado con el objeto. Esta técnica promete obtener imágenes con niveles tan bajos de iluminación como unos pocos fotones por pixel, en comparación con las decenas de miles necesarios en los sistemas convencionales [6].

Por último, un desarrollo prometedor, aunque aún en un nivel de TRL[6] bajo, es el *radar cuántico* [7]. Este se basa también en el entrelazamiento entre parejas de fotones, en este caso en el rango de las microondas, y consiste en emitir un haz de fotones compuesto por uno de los miembros de cada pareja e identificarlos entre la radiación incidente en el receptor gracias a la interacción con su compañero que hemos conservado en el equipo. Aunque se estiman necesarios todavía bastantes años de desarrollo hasta tener un equipo comercial de estas características, los resultados teóricos aseguran una mejora de la relación señal-ruido de 6dB (equivalente a un aumento del 41 % en el rango de detección máximo del radar) frente al máximo teórico obtenible con técnicas clásicas. Además, la detección podría realizarse con un flujo muy pequeño de fotones lo que permitiría permanecer indetectable al blanco.

Sensores inerciales y gravimétricos. Dentro de la capacidad de conciencia situacional, los servicios PNT (*Position-Navigation-Timing*), suministrados habitualmente por sistemas de navegación como el GPS, son básicos para el desempeño de las misiones. Sin embargo, la posibilidad de interferir la señal de GPS (mediante las técnicas denominadas *jamming* o *spoofing)*, o su indisponibilidad en entornos cerrados, ha motivado la búsqueda de soluciones independientes de los mismos. En este área,

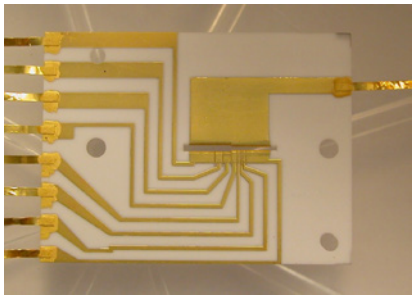

Fig. 3. Trampa de iones. (Fuente: NIST).

[5] La primera propuesta fue publicada por el físico español J. I. Cirac y el físico austriaco P. Zoller en 1995.

[6] *Technological Readiness Level* es una escala para determinar el grado de madurez de un producto o técnica, abarcando desde niveles de baja madurez (TRL 1-TRL 3) relativos a un estado de idea o prueba de concepto, hasta el TRL 9 consistente en un sistema probado con éxito en entorno real.

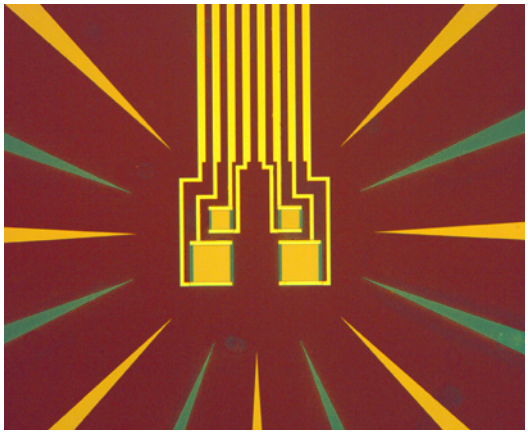

Fig. 4. Detector de fotones individuales. (Fuente: NIST).

algunos desarrollos de sensores cuánticos inerciales o gravimétricos han atraído el interés de organismos de defensa y empresas. Estos sensores se basan en celdas en las que se confina una nube de átomos gaseosos ultrafríos. A temperaturas de unas pocas millonésimas de grado sobre el cero absoluto, los átomos se encuentran en un estado cercano a la inmovilidad (por comparación, a temperatura ambiente la velocidad media de una molécula de oxígeno es de unos 500 m/s) lo que los hace muy sensibles a la inercia o a la gravedad. Esto permitiría utilizarlos como sistemas inerciales de navegación que no requerirían comunicaciones externas, y por tanto serían imposibles de interceptar, mientras que los sensores gravimétricos podrían detectar las anomalías del campo gravitatorio terrestre que previamente mapeadas constituirían una referencia precisa de la posición. Los equipos desarrollados hasta la fecha son muy voluminosos debido a las bajas temperaturas de operación, lo que requiere equipos de criogenia, y aún están en los inicios de su uso comercial, si bien en defensa podrían ser utilizados en el futuro en distintas plataformas (como por ejemplo, navales).

Sensores magnéticos. Un tipo de sensor cuántico que ha despertado mucho interés recientemente son los centros nitrógeno-vacante (NV) en diamante. Estos centros son defectos en la estructura cristalina del diamante en los que dos átomos de carbono son sustituidos por un átomo de nitrógeno, quedando una posición vacante.

El centro NV en diamante constituye un sistema cuántico con una alta sensibilidad a los campos magnéticos y eléctricos (existen desarrollos con capacidad para detectar campos magnéticos de nanoTeslas), lo que junto a otras características como su facilidad de producción, biocompatibilidad o funcionamiento a temperatura ambiente, lo postula como candidato a ser usado como sensor o *qubit*.

Aplicaciones de comunicaciones cuánticas

Las comunicaciones cuánticas consisten en la transmisión de información por canales habituales, como pueden ser fibra óptica o el espacio libre, si bien se utilizan protocolos o técnicas que aplican propiedades cuánticas de la luz. Una de las aplicaciones más maduras en este campo es la distribución cuántica de claves criptográficas (*quantum key distribution* o QKD), codificadas mediante la polarización de fotones individuales y haciendo uso del protocolo BB84 o el E91, principalmente. Estos protocolos garantizan la seguridad de la información, pues están basados en una propiedad fundamental de los sistemas cuánticos: cualquier observador que intercepte el mensaje lo alterará irremisiblemente, de forma que no podrá dejar de ser advertido por el receptor. Ya se han desplegado y puesto en operación algunas redes de comunicaciones a escala urbana (Madrid desplegó una infraestructura que integra las comunicaciones cuánticas en redes ópticas convencionales, MadQCI - *Madrid Quantum Communication Infraestructure*) e incluso China ha demostrado en 2018 la distribución cuántica de claves mediante su satélite *Micius* [8], consiguiendo generar y compartir claves a distancias superiores a 1.200 km. La distribución cuántica de claves a través del espacio libre, mediante satélite o drones, podría resultar útil en escenarios operativos. A pesar del éxito inicial, estos sistemas siguen teniendo vulnerabilidades y limitaciones. Por ejemplo, la debilidad de la señal que protege su interceptación también limita su propagación por fibra óptica más allá de pocos centenares de kilómetros, siendo necesario desarrollar repetidores cuánticos.

Aplicaciones de computación cuántica

Los ordenadores cuánticos podrían realizar determinadas operaciones mucho más rápido que un ordenador convencional debido a la característica cuántica de la superposición. Es conocido que los ordenadores clásicos codifican la información mediante *bits*. Cada *bit* puede tener dos valores (1 o 0), que corresponden a la circulación o no de electrones a través de los circuitos electrónicos. Los ordenadores cuánticos, en cambio, codifican la información en *qubits*; cada uno de estos *qubits* es un sistema cuántico que también puede tener dos estados, 0 y 1, o la superposición de ambos estados a la vez. Los *qubits* utilizados pueden ser elementos como un átomo (con un estado de energía en reposo y otro excitado) o un fotón (con dos polarizaciones distintas).

La diferencia entre los *bits* y los *qubits* es que uno de estos últimos pueden encontrarse, en un momento determinado, en una combinación de ambos *a la vez*. Esto es lo que se denomina *superposición* y es un fenómeno

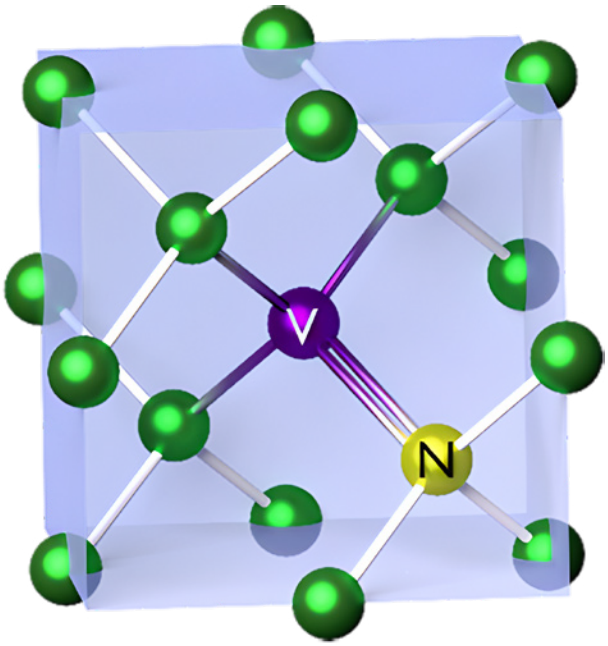

Fig. 5. Centro NV en diamante. (Fuente: NIST).

característico y sorprendente del mundo cuántico. La superposición amplía el número de estados diferentes que se pueden representar con una cantidad de *qubits*. Si con tres *bits* clásicos podemos representar cada vez uno de los 8 estados de tres *bits* posibles (000, 001, 010, 011, 100, 101, 110 y 111), con tres *qubits* podemos codificar los ocho estados simultaneamente. Esto permitirá a los ordenadores cuánticos realizar búsquedas o cálculos de optimización mucho más rápido que los ordenadores convencionales: si un ordenador clásico, para encontrar la ruta idónea entre N=1.000.000 caminos, tendrá que ir explorándolos todos sucesivamente hasta encontrar el más corto, con lo que tendrá que efectuar del orden de N/2 pasos o iteraciones, (es decir, 500.000 pasos), un computador cuántico con el número adecuado de *qubits* podrá explorar todos los caminos a la vez y solo precisará del orden de $N^{1/2}$ operaciones (1.000 iteraciones).

Algunas de las operaciones para las que se dispone ya de algoritmos implementables en ordenadores cuánticos (aunque a pequeña escala), son:

- El algoritmo de Grover que acelera las operaciones de búsqueda de bases de datos y optimización.
- El algoritmo de Shor que mejora exponencialmente la velocidad de factorización de números respecto a sus contrapartidas clásicas, lo cual es útil en criptografía.
- El algoritmo HHL que resuelve eficientemente algunos cálculos de álgebra lineal que pueden ser útiles en *machine learning*.

Aparte de los beneficios generales que puede suponer la mejora del tiempo de procesamiento en los cálculos citados, y que tendrá aplicaciones en logística, finanzas, inteligencia artificial y el modelado de sistemas complejos también aplicables en defensa, el algoritmo de Shor plantea serias amenazas pues compromete la seguridad de los sistemas de cifrado de clave pública o criptografía asimétrica. En estos sistemas, la clave pública y la clave privada es un número muy grande que se obtiene multiplicando dos números primos entre sí y se utiliza para cifrar el mensaje que solo el poseedor de los dos factores primos podrá descodificar. La seguridad de esta técnica reside en el largo tiempo que debería emplear un ordenador convencional en hacer el cálculo inverso, es decir, factorizar la clave pública. Pero esta dificultad desaparece para los ordenadores cuánticos. Se estima que un ordenador cuántico de entre 1.500 y 2.330 *qubits* que ejecutara el algoritmo de Shor podría vulnerar toda la criptografía actual (en 2019 Google presentó su ordenador cuántico Sycamore de 53 *qubits*, que ha sido superado recientemente por el Eagle de IBM con 127 *qubits*, aunque las capacidades de este último aún están por demostrar plenamente). Sin embargo, a pesar de la carrera por alcanzar las primeras aplicaciones reales en las que un ordenador cuántico supere a uno convencional, la denominada *supremacía cuántica* [10], las distintas arquitecturas físicas mediante las que se está abordando la construcción de ordenadores cuánticos, se enfrentan a retos técnicos importantes. En general, la sutileza del mundo cuántico hace a los *qubits* muy sensibles a las interferencias del entorno, destruyendo la superposición (*decoherencia*) e introduciendo errores en el procesamiento que han de ser detectados y corregidos mediente el aumento del número de *qubits*.

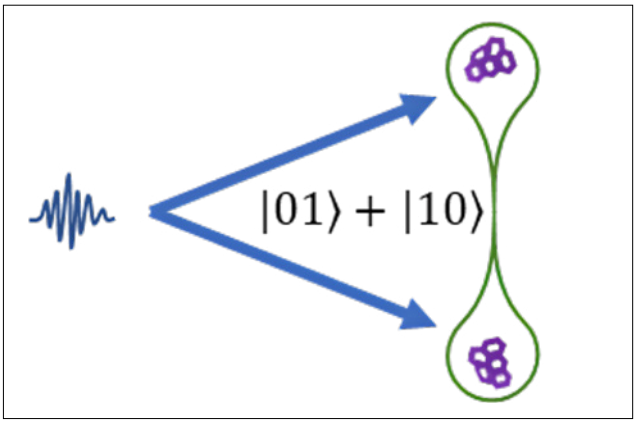

Fig. 6. Representación gráfica del principio de superposición. (Fuente: NIST).

Conclusiones

Las expectativas sobre las tecnologías cuánticas difundidas por los distintos grupos de investigación y empresas son valoradas a la vez con entusiasmo y cierto escepticismo. Existe el temor razonable de que el largo plazo necesario para que las tecnologías cuánticas se materialicen en productos y usos reales desemboque en una fase de desilusión semejante al denominado *invierno* que atravesó a la inteligencia artificial desde los años 60 del siglo pasado hasta su resurgimiento en el actual [11]. Sin embargo, la diversidad de tecnologías y aplicaciones en desarrollo asegura que, si bien no cumplan en todos los casos las altas expectativas iniciales, sí serán posibles finalmente numerosas aplicaciones que sin duda encontrarán su lugar también en la industria de defensa.

Referencias

[1] Degen C.L., Reinhard F. y Cappellaro P. (2017). *Quantum sensing*. Rev. Mod. Phys. 89. arXiv:1611.02427

[2] Bennett C.H., Brassard G. y Ekert A.K. (1992). Criptografía cuántica. Investigación y Ciencia, diciembre, 14-22.

[3] Nielsen M.A. y Chuang I.L. (2000). *Quantum computation and quantum information. Cambridge University Press*.

[4] Morsch O. y Bloch I. (2015). Mundos cuánticos simulados. Investigación y Ciencia, mayo.

[5] Genovese M. (2016). *Real applications of quantum imaging. Journal of Optics*, 18. arXiv:1601.06066

[6] Morris, P., Aspden, R., Bell, J. et al. (2015). *Imaging with a small number of photons*. Nat Commun 6, 5913. https://doi.org/10.1038/ncomms6913

[7] Barzanjeh, S., Pirandola, S., Vitali, D. y Fink, J. M. (2019). *Experimental Microwave Quantum Illumination*. arXiv quant-ph/1908.03058v1

[8] Gibney, E. (2016) *Chinese satellite is one giant step for the quantum internet.* Nature 535, 478-479. https://doi.org/10.1038/535478a

[10] Arute, F., Arya, K. y Babbush, R. et al. (2019). *Quantum supremacy using a programmable superconducting processor.* Nature 574, 505-510. https://doi.org/10.1038/s41586-019-1666-5

[11] O. Ezratty. *Mitigating the quantum hype*. (2022). https://arxiv.org/abs/2202.01925