# Computación Cuántica: Mitos y realidades

DOI: 10.29236/sistemas.n173a1

Juan G. Lalinde Pulido

Daniel Sierra Sosa

La computación cuántica ha trascendido los límites del laboratorio para convertirse en un tema central en la tecnología, la economía y la sociedad. En palabras de Isaac Chuang, profesor del MIT que trabajó con IBM en el desarrollo de los primeros computadores cuánticos, “Lo que está impulsando el entusiasmo es la verificación de que la computación cuántica es real. Ya no es el sueño de los físicos, sino la pesadilla de los ingenieros” [1].

El desarrollo de la computación cuántica ha sido un camino largo que comienza hace 100 años con la formulación de la mecánica cuánti-

ca. En 1965 Richard Feynman recibe el Premio Nobel de Física por su trabajo en electrodinámica cuántica y su relación con el espacio-tiempo [2]. En 1980, en la introducción de su libro *Computable and Uncomputable*, Manin propuso la idea de un autómata cuántico que utilizara superposición y entrelazamiento [3]. En 1981, en la conferencia *Physics of Computation* organizada por el MIT e IBM, Feynman afirmó: *'Nature is quantum, goddamn it! So if we want to simulate it, we need a quantum computer.*[1]*'* [1] [3], apoyando la idea de Manin.

A partir de estas propuestas surgen varias líneas de investigación. En 1984 se propone BB84 [4], un esquema cuántico para la distribución segura de claves criptográficas haciendo uso de propiedades cuánticas para garantizar la seguridad criptográfica, tema que luego sería desarrollado por Ekert [5]. En 1985, Deutsch demuestra que la computación cuántica es universal y equivalente a la máquina de Turing [6]. Su principal ventaja es el paralelismo masivo. Adicionalmente, en 1991, Landauer[7] muestra la relación estrecha y profunda entre la información y la física, lo que conduce a que sea natural tratar de utilizar cualquier teoría física, y especialmente la mecánica cuántica, para procesar información.

Finalmente, en los 90s se publican los dos algoritmos que mostraron la aplicabilidad de la computación cuántica y motivaron el desarrollo de los computadores cuánticos. En 1994 Peter Shor propone un algoritmo cuántico que factoriza un número en tiempo polinomial [7], que puede ser considerado el factor crítico que disparó el desarrollo de la computación cuántica por sus implicaciones para los sistemas criptográficos basados en la dificultad de la factorización y del cálculo del logaritmo discreto. En 1996, Grover publica su algoritmo que implica una aceleración cuadrática en la búsqueda de información en una colección de datos no organizados [8].

El desarrollo acelerado que tiene la computación cuántica nos ha llevado en tan solo 26 años de una primera implementación de un qubit controlable, lograda en [9], hasta los computadores cuánticos universales basados en compuertas de IBM con 1.121 qubits [10] o los computadores cuánticos especializados en *quantum annealing* de D-Wave con 5.000 qubits [11].

Ahora bien, ¿cuál es la importancia real de la computación cuántica en el mundo actual? El BID, en su informe [12], dice que *"Si bien es imposible saber con certeza cuál será su impacto social y tecnológico, se espera que haya un antes y un después de la adopción de esta nueva generación de tecnologías, tal y como ocurrió con las tecnolo-*

[1] La naturaleza es cuántica, ¡maldita sea! Así que si queremos simularla, necesitamos un ordenador cuántico.

*gías digitales"*. Por su parte, McKinsey & Company presenta en 2021 un informe sobre el ecosistema de computación cuántica [13] en el cual dice que los lideres de la industria deben comenzar a formular estrategias para la adopción de manera que puedan aprovechar las capacidades de la computación cuántica comercial. El Foro Económico Mundial, en su reporte [14], reconoce que las economías más importantes del mundo consideran la computación cuántica como una tecnología estratégica porque su potencial económico y su impacto en la economía digital las hacen estratégicas desde el punto de vista geopolítico.

Dados los avances tecnológicos de los últimos años y la importancia estratégica de la computación cuántica, es necesario que el país se prepare para poder incorporar esta tecnología a su economía. En este contexto, esta edición de la revista SISTEMAS de ACIS dedicada a la computación cuántica es una invitación a asumir el reto de la computación cuántica rigurosamente, pero sin temores. No se debe olvidar que la definición más simple de algoritmo, colección finita de pasos no ambiguos que en un tiempo finito producen un resultado, no depende de ninguna tecnología particular.

La computación cuántica es una tecnología que va a cambiar el mundo tal como lo conocemos. Este número busca ayudar a los interesados en participar activamente en este viaje hacia el futuro a comprender esta tecnología.

## Referencias


1 W. Knight, «MIT Technology Review,» 21 Febrero 2018. [En línea]. Available: https://www.technologyreview.com/2018/02/21/145300/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/. [Último acceso: 3 Diciembre 2024].

2 R. P. Feynman, «Richard P. Feynman Nobel Lecture: The Development of the Space-Time View of Quantum Electrodynamics,» 11 Diciembre 1965. [En línea]. Available: https://www.nobelprize.org/prizes/physics/1965/feynman/lecture/. [Último acceso: 3 Diciembre 2024].

3 «40 years of quantum computing,» *Nature Reviews Physics,* vol. 4, p. 1–1, 2022.

4 G. &. B. C. H. Brassard, «Quantum cryptography: Public key distribution and coin tossing,» de *International conference on computers, systems and signal processing*, Bangalore, 1984.

5 A. K. Ekert, «Quantum cryptography based on Bell's theorem,» *Physical review letters*, vol. 67, nº 6, p. 661, 1991.

6 D. Deutsch, «Quantum theory, the Church–Turing principle and the universal quantum computer,» *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, nº 1818, pp. 97-117, 1985.

7 P. W. Shor, «Algorithms for quantum computation: discrete logarithms and factoring,» de *Proceedings 35th annual symposium on foundations of computer science*, Santa Fe, 1994.

8 L. K. Grover, «A fast quantum mechanical algorithm for database search.,» de *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, Philadelphia, 1996.

9 I. L. Chuang, N. Gershendfeld y M. Kubinec, «Experimental Implementation of Fast Quantum Searching,» *Physical Review Letters*, vol. 80, nº 15, pp. 3408-3411, 1998.

10 J. Gambetta, «IBM Quantum System Two: The era of quantum utility is here,» 4 12 2023. [En línea]. Available: https://www.ibm.com/quantum/blog/quantum-roadmap-2033. [Último acceso: 3 12 2024].

11 D-Wave Quantum Inc., «The advantage quantum computer,» 2023. [En línea]. Available: https://www.dwavesys.com/solutions-and-products/systems/. [Último acceso: 3 12 2024].