# Computação Quântica: Estado Atual e Aplicações Futuras
# Quantum Computing: Current State and Future Applications

Submissão: 18/10/2024| Fim da revisão por pares: 30/10/2024| Aceite final: 04/11/2024

**Mirian Elaine Fernandes Caçula** | ETEC Professor Milton Gazzetti, Brasil | E-mail: mirian.cacula@icloud.com.br

**Resumo**

A computação quântica desponta como uma das áreas mais avançadas e promissoras da ciência e tecnologia, com potencial para revolucionar setores como criptografia, otimização e simulação de sistemas complexos. Este artigo tem como objetivo analisar o estado atual da computação quântica, incluindo suas bases teóricas, os avanços recentes e as aplicações esperadas para o futuro. Através de uma revisão detalhada das tecnologias envolvidas e dos desafios enfrentados, este estudo busca contextualizar a relevância desta nova era computacional para o progresso tecnológico global. Metodologia: revisão bibliográfica e análise de estudos de caso sobre os principais algoritmos e tecnologias da computação quântica. Resultados: identificação dos avanços atuais e das aplicações futuras. Conclusão: a computação quântica representa um caminho promissor, mas ainda enfrenta desafios significativos para sua ampla adoção.

**Palavras chaves**: Computação quântica; Criptografia quântica; Algoritmos quânticos; Tecnologias emergentes.

**Abstract**

Quantum computing emerges as one of the most advanced and promising fields in science and technology, with the potential to revolutionize sectors such as cryptography, optimization, and complex system simulation. This article aims to analyze the current state of quantum computing, including its theoretical foundations, recent advances, and future applications. Through a detailed review of the technologies involved and the challenges faced, this study seeks to contextualize the importance of this new computing era for global technological advancement.

Methodology: literature review and case study analysis on key algorithms and technologies in quantum computing. Results: identification of current advances and future applications. Conclusion: quantum computing represents a promising path, but still faces significant challenges for widespread adoption.

**Keywords:** Quantum computing; Quantum cryptography; Quantum algorithms; Emerging technologies.

## Introdução

A computação quântica emerge como um campo capaz de transformar a maneira como processamos e interpretamos informações, superando as limitações dos sistemas de computação clássicos. Fundamentada em princípios da mecânica quântica, essa tecnologia utiliza fenômenos como a superposição e o entrelaçamento para realizar cálculos com uma eficiência exponencialmente superior aos métodos tradicionais. Desde as primeiras teorias propostas por Richard Feynman e David Deutsch nos anos 1980, a computação quântica passou de conceito teórico para uma área de pesquisa com avanços práticos significativos (NIELSEN; CHUANG, 2010).

O objetivo deste artigo é examinar o estado atual da computação quântica, analisando suas principais realizações, tecnologias de base e estudos de caso que demonstram seu potencial. Além disso, são discutidas as possíveis aplicações futuras, que podem impactar setores diversos como criptografia e simulação de sistemas complexos. Entre as questões centrais abordadas estão: Quais são os principais avanços na computação quântica? Como essa tecnologia pode influenciar áreas como a segurança de dados e a simulação científica? E quais desafios técnicos precisam ser superados para que a computação quântica se torne amplamente aplicável?

## Metodologia

Para alcançar uma visão abrangente do tema, este estudo utiliza uma revisão bibliográfica, analisando publicações acadêmicas, relatórios técnicos de laboratórios de pesquisa em computação quântica e documentos de empresas líderes, como IBM, Google e D-Wave. A metodologia também inclui estudos de caso focados em



ISSN: 2676-0096 | CC BY 4.0

algoritmos fundamentais, como o de Shor para fatoração de números primos e o de Grover para busca em grandes volumes de dados. Essa abordagem permite reunir informações atuais e discutir as perspectivas para o desenvolvimento da computação quântica.

**Estado Atual da Computação Quântica**

A computação quântica, apesar de estar em fase inicial, já alcançou marcos que indicam seu potencial de transformar várias áreas da ciência e tecnologia. Em 2019, o Google anunciou a "supremacia quântica" ao utilizar seu processador Sycamore para resolver uma tarefa em 200 segundos, tempo que levaria milhares de anos para ser realizado em um supercomputador clássico (GOOGLE AI QUANTUM, 2019). Embora o conceito de supremacia quântica ainda seja debatido quanto à sua validade prática, esse feito representa um avanço significativo na capacidade de processamento.

Outro marco importante é o algoritmo de Shor, que possibilita a fatoração de números primos em tempo polinomial. Esse avanço desafia sistemas de criptografia clássicos, como o RSA, que dependem da dificuldade de fatoração como base para a segurança. Com o algoritmo de Shor, a computação quântica ameaça comprometer a segurança de dados criptografados, exigindo o desenvolvimento de sistemas de criptografia resistentes ao processamento quântico (SHOR, 1994).

O algoritmo de Grover, por sua vez, proporciona uma aceleração significativa na busca por dados não estruturados, oferecendo uma solução mais eficiente para problemas que exigem a varredura em grandes volumes de informações. Empresas como IBM estão explorando o potencial desse algoritmo para simulações químicas e otimização de funções, destacando sua aplicabilidade em cenários reais e seu impacto potencial em áreas como a farmacologia e a ciência dos materiais (BENNETT; BRASSARD, 1984).

Além disso, empresas como D-Wave e Rigetti Computing estão desenvolvendo processadores quânticos utilizando abordagens distintas, como qubits supercondutores e íons aprisionados. Cada abordagem apresenta vantagens específicas e desafios particulares, refletindo os diferentes caminhos explorados para alcançar uma computação quântica prática e escalável (RIGETTI COMPUTING, 2023).


ISSN: 2676-0096 | CC BY 4.0

**Aplicações Futuras da Computação Quântica**

A computação quântica possui um vasto potencial de aplicação em diversos setores, ainda que muitos de seus usos estejam atualmente em estágio teórico. Na área da segurança, a criptografia quântica se destaca por oferecer métodos que podem substituir os sistemas tradicionais. A criptografia pós-quântica surge como uma resposta às ameaças quânticas, desenvolvendo sistemas de segurança que resistam ao processamento em computadores quânticos. Além disso, a distribuição de chaves quânticas (QKD) proporciona uma segurança considerada inquebrável, pois utiliza princípios da mecânica quântica para proteger informações (BENNETT; BRASSARD, 1984).

A simulação de materiais é outra aplicação promissora. A computação quântica permite simular interações moleculares e processos químicos com precisão incomparável, o que pode revolucionar a descoberta de novos medicamentos, materiais e catalisadores. Pesquisas da IBM demonstraram que a simulação quântica pode representar reações químicas complexas de forma eficiente, indicando avanços significativos para a indústria farmacêutica e a ciência dos materiais (IBM, 2023).

Por fim, problemas de otimização complexa, comuns em setores como logística e finanças, podem ser resolvidos com mais eficiência pela computação quântica. A tecnologia também desperta interesse por suas possibilidades no aprimoramento de algoritmos de aprendizado de máquina e inteligência artificial, que podem ganhar velocidade e precisão com o uso de algoritmos quânticos.

## Considerações finais

Este artigo abordou os principais avanços e desafios da computação quântica, destacando sua capacidade de impactar múltiplas indústrias e promover uma transformação tecnológica. As inovações em algoritmos, como os de Shor e Grover, e o avanço nas tecnologias de hardware indicam um potencial promissor para a computação quântica. No entanto, desafios como a correção de erros, a escalabilidade


ISSN: 2676-0096 | CC BY 4.0

dos sistemas e a viabilidade prática de certas aplicações ainda limitam sua adoção em larga escala.

As aplicações futuras, especialmente em áreas como criptografia, simulação de materiais e otimização, têm o potencial de redefinir a maneira como lidamos com problemas complexos. À medida que as pesquisas avançam, é fundamental que o desenvolvimento da computação quântica ocorra de maneira ética e segura, com a colaboração entre pesquisadores, engenheiros e formuladores de políticas.

Em conclusão, a computação quântica oferece uma oportunidade única para revolucionar o processamento de informações, mas ainda enfrenta uma série de desafios técnicos e práticos. Com os avanços contínuos e uma abordagem responsável, é provável que, no futuro, essa tecnologia transforme profundamente setores inteiros da sociedade.

## Referências

BENNETT, Charles H.; BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, p. 175-179, 1984.

NIELSEN, Michael A.; CHUANG, Isaac L. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2010.

SHOR, Peter W. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, p. 124-134, 1994.

GOOGLE AI QUANTUM. Quantum supremacy using a programmable superconducting processor. Nature, v. 574, n. 7779, p. 505-510, 2019.



ISSN: 2676-0096 | CC BY 4.0