

A REVOLUÇÃO QUÂNTICA: TRANSFORMAÇÕES, DESAFIOS E POTENCIAIS DA NOVA ERA COMPUTACIONAL

THE QUANTUM REVOLUTION: TRANSFORMATIONS, CHALLENGES AND POTENTIALS OF THE NEW COMPUTATIONAL ERA

Recebido em: 30/03/2024

Aprovado em: 24/09/2024

Thiago Nelson Faria dos Reis (Orcid: <https://doi.org/0000-0002-5312-8310>)
Doutor em Ciência da Computação (UFMA). Centro Universitário Santa Terezinha - CEST.
São Luís, MA, Brasil.

Apoena Mendes Sousa (Orcid: <https://doi.org/0000-0003-4404-8842>)
Mestre em Engenharia da Computação (UEMA). Centro Universitário Santa Terezinha - CEST. São Luís, MA, Brasil.

Dadilton Bastos Melo (Orcid: <https://doi.org/0009-0000-3673-8814>)
Mestrando em Ciência da Computação (UFMA). Centro Universitário Santa Terezinha - CEST. São Luís, MA, Brasil.

Juliany Pereira Costa (Orcid: <https://doi.org/0009-0009-8937-073X>)
Mestranda em Ciência da Computação (UFMA). Centro Universitário Santa Terezinha - CEST. São Luís, MA, Brasil.

DOI: <https://doi.org/10.5281/zenodo.14058029>

Autor para correspondência:

Nome: Thiago Nelson Faria dos Reis
Endereço: Centro Universitário Santa Terezinha - CEST
E-mail: thiagonelson@cest.edu.br

RESUMO

Introdução: A computação quântica representa um avanço revolucionário na história da informática, prometendo superar as restrições dos computadores clássicos e abrir novas perspectivas em diversas áreas do conhecimento. **Objetivo:** Este artigo examina a evolução da computação quântica, desde suas bases teóricas fundamentadas nos princípios da mecânica quântica até suas possíveis aplicações em campos como criptografia, simulação de sistemas, otimização de problemas e inteligência artificial. **Materiais e Método:** A metodologia adota tem foco na revisão da literatura e na análise qualitativa, para investigar a evolução, desafios e possíveis impactos dessa tecnologia. **Resultados:** Analisamos os

principais modelos de computação quântica, seus benefícios e desafios, bem como destacamos as implicações éticas e sociais ligadas a essa tecnologia emergente. **Contribuição Científica:** Além disso, enfatizamos a importância do desenvolvimento de habilidades e programas educacionais para formar profissionais para esta nova era da informática. **Conclusão:** O artigo conclui fazendo uma reflexão sobre o impacto transformador da computação quântica na sociedade e na indústria, vislumbrando um futuro em que os limites da computação são consideravelmente expandidos.

Palavras-chave: Computação Quântica. Mecânica Quântica. Qubits. Criptografia Quântica. Inteligência Artificial Quântica.

ABSTRACT

Introduction: Quantum computing represents a revolutionary advancement in the history of computer science, promising to overcome the limitations of classical computers and open up new perspectives in various fields of knowledge. **Objective:** This article examines the evolution of quantum computing, from its theoretical foundations based on the principles of quantum mechanics to its potential applications in areas such as cryptography, system simulation, problem optimization, and artificial intelligence. **Materials and Methods:** The methodology adopted focuses on literature review and qualitative analysis, to investigate the evolution, challenges and possible impacts of this technology. **Findings:** We analyze the main models of quantum computing, their benefits and challenges, while also highlighting the ethical and social implications associated with this emerging technology. **Scientific Contribution:** Additionally, we emphasize the importance of developing skills and educational programs to train professionals for this new era in computer science. **Conclusion:** The article concludes by reflecting on the transformative impact that quantum computing will have on society and industry, envisioning a future where computational boundaries are significantly expanded.

Keywords: Quantum Computing. Quantum Mechanics. Qubits. Quantum Cryptography. Quantum Artificial Intelligence.

INTRODUÇÃO

A trajetória da computação é uma das narrativas mais empolgantes na história humana, marcada por avanços que alteram a sociedade de maneiras inimagináveis. Desde os primeiros dispositivos de cálculo, como o ábaco, passando pela invenção dos computadores digitais no século XX, até a era atual da computação clássica, o progresso tecnológico tem sido

um impulso para mudança e inovação. No entanto, com os semicondutores se aproximando de seus limites físicos e os problemas computacionais se tornando mais complexos, um novo paradigma se faz necessário (Gill *et al.*, 2022).

Nesse contexto, a computação quântica surge como uma solução promissora, capaz de ultrapassar as limitações da computação clássica. Ao contrário da computação tradicional, que utiliza bits com valores de 0 ou 1, a computação quântica emprega qubits, que, graças aos princípios da mecânica quântica, podem existir em múltiplos estados simultaneamente (Aaronson; Green, 2013). Essa superposição, aliada ao emaranhamento quântico, permite o processamento de informações de maneira muito mais rápida e complexa do que em computadores clássicos. Essa nova fronteira tem o potencial de revolucionar áreas como a criptografia e a modelagem molecular, representando um avanço significativo na nossa capacidade de compreender e processar o mundo ao nosso redor.

Este artigo examina a computação quântica como o próximo estágio da evolução tecnológica. Serão destacados seus princípios fundamentais, as possíveis aplicações, os desafios e o impacto dessa tecnologia em diversos setores. Ao explorar esse novo paradigma, buscamos compreender suas mecânicas e potenciais, além de antecipar como essa tecnologia emergente moldará o futuro da computação e influenciará, de forma mais ampla, a sociedade.

Essa análise estabelece as bases para uma investigação das inovações e dos obstáculos a serem superados, a fim de que a computação quântica alcance seu pleno potencial. A partir disso, será possível traçar uma avaliação equilibrada das perspectivas e desafios desse modelo computacional.

METODOLOGIA

Este artigo adota uma abordagem metodológica rigorosa, com foco na revisão da literatura e na análise qualitativa. O objetivo é investigar a evolução, os desafios e os impactos potenciais da computação quântica. A metodologia é dividida em várias etapas, garantindo uma compreensão abrangente do tema:

- a) **Revisão Bibliográfica:** A pesquisa é fundamentada em uma extensa revisão bibliográfica, incluindo fontes primárias e secundárias como livros, artigos de pesquisa, relatórios técnicos e teses. Isso nos permite obter insights diretos sobre o contexto histórico e teórico, além dos avanços e desafios técnicos da computação quântica. A seleção de materiais enfatiza publicações recentes e reconhecidas, assegurando a relevância e atualização das informações;
- b) **Análise de Avanços Tecnológicos:** Essa fase compreende a identificação e análise dos progressos tecnológicos recentes no campo da computação quântica. O objetivo é destacar inovações significativas, enfatizando como cada avanço contribui para superar os desafios atuais;
- c) **Exploração de Aplicações e Impactos:** A pesquisa explora possíveis usos da computação quântica em várias áreas. Através do exame de estudos de caso e previsões para compreender o impacto prático e teórico dessa tecnologia. Esta análise abrange também as consequências para a sociedade, indústria e educação, incluindo setores como segurança cibernética, saúde, finanças e outros;
- d) **Avaliação Crítica de Desafios:** Análise crítica dos desafios que a computação quântica enfrenta, abrangendo questões técnicas e éticas e barreiras à implementação prática. Este exame leva em conta discussões atuais e visões distintas no âmbito da comunidade científica e tecnológica;

e) **Síntese e Perspectivas:** Integrando os dados recolhidos, a parte final resume as principais descobertas, estabelecendo conexões com a hipótese inicial do artigo. Além disso, apresenta uma visão sobre o futuro da computação quântica ao especular sobre possíveis direções de pesquisa e desenvolvimento fundamentadas nas tendências atuais.

Esta metodologia visa fornecer uma análise detalhada e esclarecedora da computação quântica, contribuindo para o entendimento acadêmico e prático deste campo emergente e dinâmico.

COMPUTAÇÃO QUÂNTICA

Evolução da Computação

A história da computação é caracterizada por um contínuo processo de inovação, que resultou no desenvolvimento de dispositivos que gradualmente alteram nossa forma de interagir com informações e dados. Iniciou-se com equipamentos mecânicos simples, como o ábaco, utilizado há muitos anos para operações matemáticas básicas. A evolução tecnológica nos levou ao surgimento de calculadoras mais avançadas durante o século XVII, como a Pascalina criada por Blaise Pascal, capaz de realizar adições e subtrações (Aaronson, 2013; Wang, 2012; Tacchino *et al.*, 2020; Sigov; Ratkin; Ivanov, 2022).

O século XIX presenciou o desenvolvimento de máquinas mais avançadas, incluindo o motor analítico de Charles Babbage, precursor dos computadores programáveis. No entanto, foi no século XX que a computação como a conhecemos começou a se formar. A Segunda Guerra Mundial impulsionou o progresso tecnológico e resultou na criação do ENIAC em 1945, considerado um dos primeiros computadores eletrônicos digitais de uso geral.

A partir desse momento, a computação entrou em uma fase de crescimento e redução de tamanho, impulsionada pela criação do transistor na década de 1940 e, posteriormente, pela incorporação de circuitos que permitiu o surgimento dos microprocessadores nos anos de 1970. Esses desenvolvimentos marcaram o começo da era dos computadores pessoais, tornando a tecnologia computacional mais acessível e preparando o terreno para a revolução digital subsequente (Aronson, 2013; Wang, 2012; Tacchino *et al.*, 2020; Sigov; Ratkin; Ivanov, 2022).

Nos anos seguintes, a computação convencional progrediu em um ritmo sem precedentes, impulsionada pela Lei de Moore, que previu o dobro do aumento do número de transistores em microprocessadores a cada dois anos, resultando em uma crescente exponencial da capacidade de processamento (Silva, 2020; Quais; Moore, 2022). Este período testemunhou o surgimento da internet, a ampliação do uso de computadores pessoais e o desenvolvimento de smartphones, transformando drasticamente nosso modo de vida, trabalho e comunicação.

Atualmente, apesar do grande poder dos computadores modernos, eles começam a enfrentar limitações físicas e teóricas em sua capacidade de processamento, especialmente para tarefas que requerem grandes quantidades de cálculos paralelos ou que superam as capacidades dos algoritmos tradicionais. É nesse contexto, a computação quântica se apresenta capaz de superar esses limites, ao explorar os princípios inexplicáveis e fascinantes da mecânica quântica, e iniciar assim um novo capítulo na evolução da computação (Rajak *et al.*, 2023; Dunjko; Wittek, 2020; Garg; Ramakrishnan, 2020).

Um Novo Paradigma: Computação Quântica

A transição para a computação quântica é mais do que um avanço tecnológico. Ela representa uma mudança profunda no paradigma computacional. Enquanto a computação clássica utiliza bits com valores fixos, como 0 ou 1, a computação quântica introduz os qubits. Esses qubits desafiam nossa compreensão tradicional, operando em estados de superposição. Isso significa que um qubit pode representar 0, 1 ou qualquer estado intermediário simultaneamente (Abdelgaber; Nikolopoulos, 2020; Aguado; Kouwenhoven, 2020).

Essa particularidade dos qubits é resultado dos princípios fundamentais da mecânica quântica - superposição e emaranhamento. A superposição permite que os qubits realizem múltiplos cálculos ao mesmo tempo, o que poderia trazer avanços significativos em velocidade em comparação com os computadores clássicos para determinados problemas computacionais. O emaranhamento quântico, outro fenômeno exclusivo, possibilita a conexão de qubits em diferentes locais de tal forma que o estado de um (independentemente da distância) pode depender instantaneamente do estado do outro, introduzindo um novo nível de complexidade e interconexão sem similar na computação clássica.

A computação convencional, com seu modelo previsível e linear, tem sido útil, impulsionando avanços em todas as áreas do conhecimento humano. No entanto, ela enfrenta limitações inerentes ao lidar com problemas que crescem exponencialmente ou têm natureza intrinsecamente quântica, como a simulação de sistemas moleculares ou a otimização de grandes conjuntos de dados. Nesse contexto, a computação quântica promete uma revolução não apenas na velocidade de processamento, mas também em uma nova abordagem para interpretar e processar informações (Roy *et al.*, 2020; Wu *et al.*, 2021; Herman *et al.*, 2022).

De acordo com Gill *et al.* (2022); McArdle *et al.*, 2020; Wang, 2012), ao adotar os princípios quânticos, a computação quântica não está apenas se estabelecendo como sucessora da computação clássica; ela está

definindo um novo caminho para o conceito de computação. Este novo paradigma oferece diversas possibilidades que podem transformar áreas como criptografia, pesquisa farmacêutica, inteligência artificial e muito mais, indicando que a computação quântica não representa apenas uma evolução gradual, mas sim uma mudança fundamental na forma como lidamos com informações em seu nível mais elementar.

Conceitos Básicos da Mecânica Quântica e Computação Quântica

Os conceitos fundamentais apresentados nesta seção são baseados nos princípios da mecânica quântica, uma teoria científica desenvolvida para explicar o comportamento de partículas em escalas atômicas e subatômicas. A computação quântica, em particular, baseia-se em dois pilares essenciais dessa teoria: a superposição e o emaranhamento quântico.

As explorações e análises aqui apresentadas são respaldadas por uma série de estudos e pesquisas realizadas por McArdle *et al.* (2020), Wu *et al.* (2021), Rajak *et al.* (2023), Garg e Ramakrishnan (2020), Dunjko e Wittek (2020), Aguado e Kouwenhoven (2020) e Gill *et al.* (2022).

Superposição Quântica

Superposição é um princípio fundamental da mecânica quântica. Ele permite que uma partícula, como um elétron ou um fóton, exista em múltiplos estados ao mesmo tempo. Aplicado aos qubits, isso significa que um único qubit pode representar simultaneamente 0, 1 ou uma combinação desses estados. Esse comportamento é o que possibilita aos computadores quânticos realizarem cálculos paralelos com muito mais eficiência do que os sistemas clássicos. Permitindo, por exemplo, a realização de grandes quantidades de cálculos em paralelo, potencializando exponencialmente as buscas e o processamento de dados.

Emaranhamento Quântico

O emaranhamento é outro fenômeno quântico que desafia a intuição, permitindo que as partículas se conectem de tal maneira que o estado de uma partícula influencie instantaneamente o estado de outra, independente da distância entre elas. No contexto da computação quântica, isso significa que qubits emaranhados podem correlacionar seus estados de forma não encontrada na computação clássica. O emaranhamento possibilita um novo tipo de processamento paralelo e comunicação instantânea entre qubits, explorável para realizar cálculos complexos com mais eficiência e resolver problemas demasiadamente difíceis para os computadores clássicos.

Aplicações na Computação Quântica

Esses princípios da mecânica quântica são utilizados na computação quântica para executar funções como a quebra de números grandes, pesquisa em bases de dados e simulação de sistemas quânticos, que são atividades fundamentais em áreas como criptografia, ciência dos materiais e física. A exploração da superposição e do entrelaçamento em algoritmos quânticos proporciona uma nova abordagem para o processamento de informações, consagrando a computação quântica como um avanço paradigmático em comparação com as capacidades da computação clássica.

Ao compreender esses princípios fundamentais, é possível apreciar mais claramente o potencial revolucionário da computação quântica e como ela visa ampliar os limites do que é computacionalmente viável, sinalizando o começo de uma nova era na história da tecnologia computacional.

Diferenças entre Qubits e Bits Clássicos

A distinção fundamental entre qubits e os bits clássicos reside no que torna a computação quântica tão poderosa e diferente da computação clássica. Enquanto os bits são a base da computação tradicional, representando a menor unidade de dados em sistemas digitais com seus

dois valores possíveis (0 ou 1), os qubits possuem propriedades únicas que possibilitam um processamento e armazenamento de informações mais avançados, o que fundamenta toda a operacionalidade quântica.

Em contrapartida, os qubits funcionam com base nos princípios da mecânica quântica, exibindo propriedades que não têm equivalentes no universo clássico, detalhadas a seguir:

- **Superposição:** Enquanto um bit está sempre em um estado de 0 ou 1, um qubit pode existir em um estado de superposição que engloba tanto o 0 quanto o 1, além de todos os pontos intermediários simultaneamente. Essa característica possibilita que um único qubit represente muito mais informação do que um bit e permite aos computadores quânticos realizar cálculos em múltiplos estados potenciais ao mesmo tempo;
- **Emaranhamento:** Quando os qubits se entrelaçam, o estado de um qubit não pode ser descrito isoladamente do estado de outro, não importa a distância que os separa. Essa conexão permite que os qubits compartilhem informações instantaneamente e é uma propriedade utilizada pelos computadores quânticos para realizar tarefas complexas de forma mais eficiente do que os computadores clássicos;
- **Probabilidade e Colapso de Estado:** Uma diferença importante está na medição: ao contrário de um bit, cuja medição sempre revela o mesmo valor que ele representa (0 ou 1), a medição de um qubit em superposição causa o colapso do seu estado para 0 ou 1 com uma certa probabilidade. Isso indica que o resultado da medida de um qubit é essencialmente probabilístico, refletindo a natureza probabilística da mecânica quântica;
- **Capacidade de Processamento:** Essas discrepâncias se refletem em uma capacidade de processamento significativamente maior para os computadores quânticos. Por exemplo, onde dois bits

clássicos podem estar em um dos quatro estados possíveis a qualquer momento, dois qubits podem existir em uma superposição desses mesmos quatro estados simultaneamente - o que gera um aumento exponencial na quantidade de informação que pode ser processada à medida que mais qubits são adicionados.

Em resumo, os qubits se distinguem dos bits clássicos por suas propriedades fundamentais e pela forma como processam informações, abrindo caminho para avanços computacionais que vão além das capacidades dos sistemas baseados em bits. Essas discrepâncias são o que permitem à computação quântica o potencial de resolver problemas complexos que são inacessíveis ou demasiadamente lentos para serem solucionados por computadores clássicos, inaugurando uma nova era na evolução da tecnologia computacional.

Desenvolvimento da Computação Quântica

A computação quântica é uma área de estudo que combina os conceitos da mecânica quântica com a teoria da informação, com o objetivo de construir uma nova geração de computadores. Este resumo descreve alguns dos eventos importantes e contribuições significativas que influenciaram o avanço da computação quântica, segundo Shara (2023), Sahoo *et al.* (2020), Fox, Zwickl e Lewandowski (2020), Cuomo, Caleffi e Cacciapuoti (2020) e Araújo-Moreira *et al.* (2023).

- **Início Conceitual**

- Décadas de 1960 e 1970: O conceito de computação quântica começou a se desenvolver com pesquisadores como Richard Feynman e Yuri Manin, que sugeriram que os fenômenos quânticos poderiam ser explorados para realizar cálculos. Especialmente em 1982, Feynman propôs que um computador

quântico teria maior eficácia na simulação de sistemas quânticos em comparação aos computadores clássicos.

- **Desenvolvimento Teórico**

- 1985: David Deutsch, da Universidade de Oxford, propôs a concepção do primeiro computador quântico universal, marcando um avanço ao desenvolver um modelo capaz de emular qualquer processo físico;
- 1994: Um marco crucial ocorreu quando Peter Shor, do MIT, criou o algoritmo de Shor. Esse algoritmo demonstrou que um computador quântico poderia realizar a fatoração de números grandes de forma exponencialmente mais rápida do que os melhores algoritmos conhecidos em um computador clássico, trazendo implicações significativas para a área da criptografia.

- **Primeiros Experimentos e Implementações**

- Década de 1990: Os primeiros modelos de computadores quânticos foram desenvolvidos, utilizando diferentes sistemas quânticos, como ressonância magnética nuclear e armadilhas de íons;
- 2001: A IBM e o MIT demonstraram o algoritmo de Shor em um computador quântico de 7 qubits, usando a fatoração do número 15 como prova de conceito.

- **Avanços Recentes**

- Década de 2000 em diante: A pesquisa no campo da computação quântica tem avançado rapidamente, com progressos em coerência quântica, escalabilidade e algoritmos. Grandes empresas como Google, IBM e outras têm feito esforços significativos para aprimorar a tecnologia de computadores quânticos visando torná-los mais poderosos e práticos;

- 2019: O Google revelou que seu processador quântico Sycamore atingiu a "dominação quântica" ao completar um cálculo específico que seria inviável em um supercomputador clássico, embora esse feito tenha sido motivo de discussão na comunidade científica.

Desde as bases teóricas até os primeiros modelos experimentais e os avanços recentes em direção à computação quântica tem progredido a um ritmo impressionante. Pesquisadores renomados e colaborações globais seguem explorando o amplo potencial dessa tecnologia, apontando para um futuro promissor.

Modelos de Computação Quântica

A computação quântica engloba diferentes tipos de modelos que se diferenciam na forma como manipulam e processam informações em sistemas quânticos. Cada modelo possui suas próprias características distintas, benefícios e desafios. Nesta seção, são analisados e comparados os principais modelos de computação quântica, com o intuito de proporcionar uma compreensão mais aprofundada das diferenças entre eles e seus possíveis usos, de acordo com Sahoo *et al.* (2020), Cuomo, Caleffi e Cacciapuoti (2020), Ollitrault, Miessen e Tavernelli (2021), Wang (2012) e McArdle *et al.* (2020), Gill *et al.* (2022), Smith *et al.* (2022) e Zhang *et al.* (2020).

- **Modelo de Circuito Quântico:** O modelo de circuito quântico é o mais clássico e extensivamente pesquisado, envolvendo a aplicação sequencial de portas quânticas que modificam o estado de qubits individuais ou múltiplos qubits simultaneamente.
 - Vantagens: É amplamente compreendido e tem sido fundamental para a maioria dos algoritmos quânticos desenvolvidos até agora, como o algoritmo de Shor e o algoritmo de Grover;

- Desafios: São necessários controles precisos dos qubits e métodos eficientes de correção de erros para enfrentar a decoerência e outros ruídos quânticos.
- **Computação Quântica Adiabática:** Este modelo é operado com base no princípio da evolução adiabática, em que um sistema quântico que começa em seu estado fundamental passa por uma transformação lenta e contínua para garantir que permaneça nesse estado.
 - Vantagens: Sua natureza gradual e adiabática pode torná-lo potencialmente mais resistente a certos tipos de erros quânticos;
 - Desafios: Pode ser mais lento do que o modelo de circuito quântico e é principalmente apropriado para problemas de otimização.
- **Computação Topológica Quântica:** Baseia-se na utilização de qualquerons, que são partículas quânticas com estatísticas não abelianas, para efetuar cálculos. A informação é armazenada nas características topológicas dos estados quânticos, o que a torna intrinsecamente resistente a erros locais.
 - Vantagens: Oferece uma grande resistência a falhas, uma vez que os dados não são armazenados em locais específicos, mas sim nas propriedades globais do sistema;
 - Desafios: A aplicação prática é altamente exigente, requerendo condições experimentais específicas que são difíceis de atingir.
- **Computação Quântica Baseada em Medidas:** Neste modelo, a computação é conduzida através de uma série de medições em um estado quântico altamente entrelaçado, chamado de estado cluster. A ordem e o tipo das medições determinam o algoritmo executado.

- Vantagens: Permite uma abordagem modular que pode ser potencialmente expandida para a computação quântica;
- Desafios: A preparação precisa de estados cluster altamente emaranhados e o controle das medições são requisitos essenciais.

Cada tipo de computação quântica tem suas próprias vantagens e desafios exclusivos, o que torna alguns modelos mais apropriados para resolver tipos específicos de problemas ou aplicações. A escolha do modelo pode depender do objetivo da computação, das restrições tecnológicas e do contexto operacional. Conforme avança a tecnologia quântica, compreender e integrar esses diferentes modelos se tornará fundamental para o desenvolvimento de computadores quânticos versáteis e potentes.

APLICAÇÕES DA COMPUTAÇÃO QUÂNTICA

Potenciais Aplicações da Computação Quântica

A computação quântica, com suas capacidades singulares provenientes da mecânica quântica, tem o potencial de revolucionar diversas áreas, proporcionando respostas para desafios complexos que atualmente os computadores clássicos não conseguem enfrentar. A seguir, examinamos como essa tecnologia emergente pode influenciar setores importantes como criptografia, solução de problemas complexos, simulação de sistemas quânticos e inteligência artificial.

- **Criptografia**

A computação quântica representa tanto um desafio quanto uma oportunidade para o campo da criptografia. Com o algoritmo de Shor, os computadores quânticos têm a capacidade de quebrar sistemas criptográficos atualmente seguros, como a criptografia RSA, que depende da complexidade de fatorar grandes números primos. Isso poderia

transformar profundamente a segurança cibernética, demandando a criação de novos métodos de criptografia capazes de resistir aos ataques quânticos. Além disso, a computação quântica também possibilita o desenvolvimento da criptografia quântica, que utiliza o emaranhamento quântico para criar chaves virtualmente invioláveis e elevar o nível de segurança das comunicações (Vazquez; Pantarotto; Battilana, 2021).

- **Otimização de Problemas**

Muitos desafios em áreas como logística, finanças e engenharia envolvem a eficiência na utilização de recursos, o que pode se tornar consideravelmente mais complexo à medida que o escopo do problema aumenta. Algoritmos quânticos, como o Quantum Approximate Optimization Algorithm, propõem resolver tais desafios de forma mais eficiente do que os algoritmos clássicos. Isso poderia resultar em avanços significativos na maneira como planejamos rotas de transporte, gerenciamos portfólios de investimento ou desenvolvemos novos materiais (Dunjko; Wittek, 2020; Xin *et al.*, 2020; Herman *et al.*, 2022).

- **Simulação de Sistemas Quânticos**

Uma das aplicações mais promissoras da computação quântica é a simulação de sistemas quânticos, algo que Richard Feynman já havia previsto nas primeiras décadas desse campo. Os computadores quânticos podem modelar sistemas quânticos complexos de forma mais natural e eficiente do que os computadores clássicos, uma vez que operam com base nos mesmos princípios quânticos. Isso tem implicações significativas para a química e a física, permitindo aos cientistas desvendar os segredos das reações químicas, desenvolver novos materiais com propriedades específicas e compreender melhor os fenômenos físicos em escala quântica (McArdle *et al.*, 2020; Rajak *et al.*, 2023; Ollitrault; Miessen; Tavernelli, 2021).

- **Inteligência Artificial e Aprendizado de Máquina**

A computação quântica tem o potencial de revolucionar a inteligência artificial e o aprendizado de máquina, oferecendo novas abordagens para processar e analisar grandes conjuntos de dados. Algoritmos quânticos de aprendizado de máquina podem realizar tarefas como classificação e identificação de padrões com maior rapidez e eficiência em comparação com seus equivalentes clássicos. Isso pode resultar em avanços nas áreas como diagnóstico médico, previsão do mercado financeiro, e até mesmo no desenvolvimento de novas formas de IA (Vazquez; Pantarotto; Battilana, 2021; Schuld; Killoran, 2022; Cerezo et al., 2022).

- **Resolvendo Problemas Intratáveis com a Computação Quântica**

A computação quântica tem o potencial de transformar a abordagem de problemas considerados intratáveis para os computadores clássicos. Esses problemas têm uma complexidade que cresce exponencialmente com o tamanho do sistema, tornando-se impraticáveis para solução em um tempo razoável, mesmo com os supercomputadores mais avançados (Dunjko; Wittek, 2020; Abdelgaber; Nikolopoulos, 2020; AbuGhanem; Eleuch, 2023).

Ou seja, na computação clássica, alguns problemas aumentam exponencialmente, o que quer dizer que o tempo necessário para resolvê-los cresce de acordo com o tamanho do problema. Por exemplo, otimização combinatória, simulação de sistemas quânticos e certos tipos de criptografia. Com a superposição, um computador quântico pode realizar cálculos em vários estados simultaneamente. Ao contrário de um computador clássico que processa uma sequência de operações em um conjunto único de dados por vez.

- **Algoritmos Quânticos Específicos**

Segundo (Cuomo; Caleffi; Cacciapuoti, 2020; Gill et al., 2022; Ollitrault; Miessen; Tavernelli, 2021), o impacto da computação quântica na

sociedade atual pode ser confirmado por meio de dois exemplos de algoritmos clássicos utilizados, conforme descrito a seguir:

- Algoritmo de Shor: Talvez o exemplo mais conhecido seja o algoritmo de Shor, que é capaz de fatorar números grandes muito mais rapidamente do que os melhores algoritmos clássicos, numa escala exponencial. Isso tem um impacto significativo na criptografia, área baseada na complexidade da fatoração de grandes números primos no tempo disponível.
- Algoritmo de Grover: Para pesquisar em uma base de dados não estruturada, o algoritmo de Grover proporciona um aumento quadrático na velocidade, significando que um problema que requereria N operações em um sistema clássico exigiria apenas \sqrt{N} operações em um sistema quântico.

As possíveis aplicações da computação quântica são extensas e podem influenciar virtualmente todos os setores da sociedade e da economia global. Apesar de ainda estarmos nas fases iniciais da implementação prática dessas aplicações, o rápido progresso na pesquisa e no desenvolvimento nesse campo indica que a computação quântica tem o potencial de se tornar uma tecnologia revolucionária, redefinindo as fronteiras do possível em termos de computação e análise de dados.

DESAFIOS E LIMITAÇÕES

Desafios da Computação Quântica

Apesar do grande potencial da computação quântica, a concretização prática dessa tecnologia enfrenta desafios técnicos e teóricos significantes. Questões como decoerência, escalabilidade, controle de erros e outros obstáculos técnicos são foco das pesquisas atuais para permitir que os computadores quânticos se tornem uma realidade funcional e confiável. De acordo com (Vazquez; Pantarotto;

Battilana, 2021; Schuld; Killoran, 2022; Cerezo *et al.*, 2022; Wu *et al.*, 2021; AbuGhanem; Eleuch, 2023; Roy *et al.*, 2020; Zhang *et al.*, 2020; Gill *et al.*, 2022), seguem os principais desafios:

- **Decoerência Quântica**

A decoerência é possivelmente o desafio mais proeminente no avanço dos computadores quânticos. Refere-se à perda de informações quânticas dos qubits devido a interações involuntárias com o ambiente externo. Estas interações fazem com que os qubits percam seu estado de superposição ou emaranhamento, fundamentais para a computação quântica, e retornem a um estado clássico. Lidar com a decoerência exige isolamento extremo do sistema quântico e técnicas sofisticadas para manter a coerência quântica por tempo suficiente para realizar cálculos relevantes.

Diversas pesquisas têm sido realizadas para investigar diferentes métodos de prolongar a coerência dos qubits, tais como o aprimoramento das técnicas de isolamento e a criação de novos materiais e designs que reduzem ao máximo a interação com o ambiente. Além disso, estão em estudo abordagens mais eficientes para corrigir ativamente os erros quânticos à medida que ocorrem, sem comprometer as informações quânticas.

- **Escalabilidade**

Protótipos e computadores quânticos iniciais demonstram a viabilidade da tecnologia com um número limitado de qubits, mas a escalabilidade representa um desafio significativo. Aumentar o número de qubits é crucial para que a computação quântica alcance seu potencial teórico. No entanto, conforme o número de qubits aumenta, a complexidade do sistema e as dificuldades em manter coerência quântica se tornam mais intensas. Desenvolver sistemas capazes de controlar, entrelaçar e ler corretamente um grande número de qubits sem perda de estabilidade é uma das principais barreiras para o avanço desta tecnologia.

Pesquisadores estão trabalhando em novas estruturas de hardware e métodos de produção que podem integrar um maior número de qubits com eficiência. Isso envolve aprimorar as conexões entre os qubits e explorar novos tipos que possam ser dimensionados com mais facilidade.

- **Controle de Erros Quânticos**

A correção de erros é um elemento crucial na computação clássica, mas na computação quântica, este conceito enfrenta novas complexidades. Devido à natureza delicada dos qubits e à probabilidade de ocorrência de erros durante as operações quânticas, é fundamental desenvolver métodos eficazes para a correção desses erros. Esses métodos devem ser capazes de detectar e corrigir os erros sem perturbar a informação quântica, uma tarefa conhecida por sua dificuldade decorrente do princípio da medição quântica, que pode alterar o estado do sistema.

O progresso na correção de erros dos algoritmos avançados e o aprimoramento da precisão dos pulsos e campos magnéticos ou elétricos empregados na manipulação dos qubits são algumas das abordagens para aumentar a fidelidade. Adicionalmente, estabelecer benchmarks e padrões rigorosos será útil para avaliar e impulsionar melhorias na precisão das operações quânticas.

- **Fidelidade e Conectividade**

A precisão das operações quânticas, que se refere à exatidão com que essas operações são realizadas, é fundamental para o desempenho eficiente de um computador quântico. Além disso, a habilidade de interligar computadores quânticos em uma rede, possibilitando a comunicação e compartilhamento de informações quânticas à distância, ainda está em fase de desenvolvimento.

Está em andamento o desenvolvimento de tecnologias para estabelecer redes quânticas, que envolvem a implementação de repetidores quânticos com o objetivo de manter a integridade do estado

quântico das informações durante a transmissão, além da integração dos sistemas quânticos com as tecnologias já existentes em telecomunicações.

- **Integração e Programação**

Desenvolver uma estrutura quântica que possa ser eficientemente integrada e expandida, juntamente com o avanço de linguagens de programação e algoritmos adequados para esta nova forma de computação, representa outro desafio substancial. A ligação entre a tecnologia quântica e os utilizadores finais, através do software, deve ser suficientemente sólida e acessível para possibilitar a completa exploração das capacidades quânticas.

A disponibilidade de computadores quânticos através da computação em nuvem possibilita um acesso mais abrangente, tornando a pesquisa e o desenvolvimento em computação quântica mais acessíveis. Ao mesmo tempo, o avanço de interfaces de programação mais intuitivas e ferramentas educacionais está simplificando a entrada de novos profissionais nesse campo.

O desenvolvimento de computadores quânticos apresenta desafios significativos, porém as pesquisas contínuas e os avanços nesse campo são promissores. À medida que esses obstáculos são superados, espera-se que a tecnologia quântica se torne cada vez mais viável, abrindo novos horizontes para sua aplicação em diversas áreas do conhecimento.

IMPACTO DA COMPUTAÇÃO QUÂNTICA NA SOCIEDADE E NA INDÚSTRIA

A computação quântica, com a promessa de realizar cálculos exponencialmente mais rápidos e resolver problemas complexos, tem o potencial de causar mudanças significativas em diversas áreas da sociedade e da indústria. Ao examinarmos seu impacto, é crucial considerar várias esferas, como a segurança cibernética, progressos científicos e inovação tecnológica.

Conforme destacado por Ollitrault, Miessen e Tavernelli (2021), Cuomo, Caleffi e Cacciapuoti (2020), Shara (2023) e Sahoo *et al.* (2020), os setores mais impactados incluem:

A computação quântica apresenta desafios e oportunidades para a segurança cibernética. Por um lado, sua capacidade de quebrar criptografias atuais pode representar uma ameaça à segurança dos dados e das comunicações. Algoritmos como o de Shor têm o potencial de decifrar sistemas atualmente considerados seguros, o que poderia resultar em uma reorganização completa da segurança cibernética global.

Em reação a isso, tanto a indústria quanto os governos e pesquisadores estão investindo em criptografia pós-quântica, que previne ataques de computadores quânticos e assegura a proteção de informações delicadas e infraestruturas críticas. Outros domínios afetados nesse cenário incluem o blockchain e a segurança de dados, já que a computação quântica também pode impactar essas tecnologias, demandando novas abordagens para garantir integridade e segurança nas transações e registros.

Por outra perspectiva, a capacidade dos computadores quânticos de emular sistemas complexos pode acelerar consideravelmente a investigação em áreas como física, química e biologia. Ao simular moléculas e materiais em nível quântico, é possível avançar no desenvolvimento de novos fármacos e materiais com propriedades inovadoras, impulsionando progressos na área da medicina e na indústria. Além disso, esses computadores podem ser empregados para resolver enigmas desafiadores da física teórica e auxiliar na análise de enormes conjuntos de dados nas pesquisas espaciais, abrindo assim novas possibilidades para compreender o universo.

A influência e a transformação na indústria também são dignas de menção, pois introduzem eficiências e capacidades nunca antes vistas. Por exemplo, nos setores de logística, finanças e manufatura, a computação

quântica pode aprimorar processos, diminuindo os custos e aumentando a eficiência.

As maiores beneficiadas pela computação quântica são, talvez, a Inteligência Artificial e o Big Data. A capacidade de processar e analisar grandes volumes de dados tem o potencial para revolucionar essas áreas, fornecendo insights mais abrangentes e impulsionando a inovação em vários setores.

Questões Éticas e Sociais na Computação Quântica

A evolução da computação quântica não só traz avanços tecnológicos, mas também levanta diversas considerações éticas e sociais significativas. Conforme essa tecnologia progride, é essencial analisar as possíveis repercussões na sociedade para garantir que seu desenvolvimento e uso sejam feitos de forma responsável e justa (Malikovich; Tashev; Safoev, 2023; Perrier, 2021; Cuomo; Caleffi; Cacciapuoti, 2020).

Conforme os autores citados, a computação quântica tem o potencial de comprometer a segurança das criptografias atuais, colocando em risco a privacidade e a confidencialidade dos dados. Isso levanta questões éticas sobre como proteger informações pessoais e sensíveis. É fundamental criar novos padrões de criptografia que sejam resistentes à computação quântica para garantir a privacidade individual e manter a integridade dos dados na era pós-quântica.

Uma outra consideração ética levantada é a possibilidade de que o acesso à computação quântica se torne uma questão significativa de disparidade, na qual apenas certos grupos ou países com recursos adequados poderiam tirar proveito dessa nova tecnologia. É crucial lidar com as questões de justiça no acesso à computação quântica para impedir o aumento da lacuna digital e assegurar a ampla partilha dos seus benefícios.

Da mesma forma, as aplicações militares e estratégicas da computação quântica, especialmente em áreas como criptografia e logística, suscitam questões éticas sobre a corrida armamentista e a estabilidade global. É crucial promover o desenvolvimento responsável e regular a tecnologia quântica em contextos militares e estratégicos para evitar escaladas de conflitos e fomentar a paz.

De maneira semelhante às questões éticas relacionadas à inteligência artificial, a computação quântica também traz à tona preocupações sobre o impacto no mercado de trabalho. A automação e otimização avançadas pela computação quântica podem remodelar setores da economia e do mercado de trabalho, possivelmente deslocando trabalhadores e gerando necessidades significativas de requalificação. É essencial considerar e planejar para as transições de carreira e oportunidades de desenvolvimento profissional em um cenário onde a computação quântica assume um papel central.

As implicações éticas e sociais relacionadas à computação quântica são igualmente relevantes aos avanços tecnológicos nesta área. Ao explorarmos este novo campo, é essencial assegurar que os progressos na computação quântica estejam em sintonia com princípios éticos, fomentando uma sociedade mais equitativa, segura e inclusiva. Isto exige a colaboração entre cientistas, legisladores, indústrias e a comunidade para moldar um futuro no qual a tecnologia quântica beneficie todos sem comprometer os direitos ou o bem-estar de indivíduos e grupos sociais.

A Educação na era da Computação Quântica

A computação quântica está emergindo como um campo revolucionário, com um potencial imenso para transformar diversas indústrias. Como apontam Nita *et al.* (2023), Fox, Zwickl e Lewandowski (2020), Rasa, Palmgren e Laherto (2022), e Cuomo, Caleffi e Cacciapuoti (2020), há uma necessidade crucial de cultivar uma nova geração de

profissionais através do desenvolvimento de talentos e programas educacionais especializados. Baseado nestas fontes, esta seção explora a importância do desenvolvimento de habilidades e da educação específica em computação quântica, discutindo estratégias para formar uma força de trabalho qualificada e bem-informada, pronta para liderar inovações futuras.

Necessidade de Especialistas em Computação Quântica: À medida que a computação quântica se torna mais próxima da aplicação prática, a procura por profissionais qualificados está crescendo. Existe uma demanda crescente por cientistas, engenheiros e técnicos com um conhecimento profundo em mecânica quântica, algoritmos quânticos, design de sistemas quânticos e programação para o ambiente quântico.

Criação de Programas Educacionais: Universidades e instituições de ensino estão criando cursos, certificações e programas de graduação especializados em computação quântica. Esses programas têm como objetivo fornecer uma base sólida nos princípios da física quântica, ao mesmo tempo que abordam aplicações práticas e habilidades de programação. A colaboração entre instituições acadêmicas e a indústria é crucial para alinhar a educação com as demandas do mercado, garantindo assim que os currículos sejam pertinentes e que os estudantes tenham oportunidades de adquirir experiência prática.

Fomento da Pesquisa e Inovação: Programas de mestrado, doutorado e parcerias em pesquisa entre universidades e empresas são fundamentais para impulsionar a inovação na área da computação quântica. Investimentos nessa área contribuem para o avanço do conhecimento científico e o desenvolvimento de novas tecnologias. Iniciativas de pesquisa promovem a colaboração interdisciplinar, reunindo especialistas em física, ciência da computação, engenharia e matemática – algo essencial para superar os desafios complexos associados à computação quântica.

Educação Continuada e Treinamento Profissional: Além da educação formal, é crucial investir em programas de aprendizado contínuo e treinamento profissional para manter os conhecimentos atualizados frente aos avanços rápidos no campo da computação quântica. Participar de workshops, seminários online e cursos intensivos pode ser uma maneira eficaz de garantir que os profissionais estejam por dentro das mais recentes tecnologias e práticas do setor.

Diversidade e Inclusão: É crucial fomentar a diversidade e a inclusão no âmbito da computação quântica. Atrair e apoiar talentos de origens diversas pode impulsionar a inovação, trazendo perspectivas variadas e soluções criativas para os desafios do setor. Iniciativas voltadas à incorporação de mulheres, minorias e grupos sub-representados em STEM podem enriquecer consideravelmente o ambiente de pesquisa e indústria.

Preparando a Próxima Geração: A inclusão da computação quântica em estágios mais iniciais de educação, como o ensino médio e disciplinas introdutórias na graduação, tem o potencial de despertar interesse e preparar os alunos para futuras carreiras nesse domínio. Programas educacionais que visam aumentar a compreensão sobre a computação quântica e suas aplicações podem motivar jovens estudantes a seguir caminhos profissionais nessa área, assegurando um constante fluxo de talentos renovado.

O crescimento de habilidades e o ensino da computação quântica são essenciais para aproveitar totalmente o potencial desta tecnologia inovadora. Investir na capacitação de especialistas qualificados e no estabelecimento de um ambiente educacional sólido são passos cruciais rumo à liderança das futuras inovações, assegurando que a computação quântica alcance seu impacto transformador na sociedade e indústria.

CONCLUSÃO

A computação quântica representa uma transformação significativa na tecnologia, alterando profundamente a maneira como problemas computacionais são abordados. Ao longo deste artigo, discutimos como os qubits e os princípios quânticos, como superposição e emaranhamento, trazem uma nova perspectiva para a informática, permitindo o processamento paralelo de informações em uma escala sem precedentes. Esse avanço tecnológico tem potencial para impactar de forma marcante setores como a criptografia, a simulação de sistemas complexos e a inteligência artificial.

A importância da computação quântica abrange diversas áreas, desde a capacidade de quebrar criptografias atualmente consideradas seguras, desafiando a reinvenção da segurança cibernética, até a habilidade de simular sistemas quânticos complexos. Isso abre novas possibilidades para avanços científicos em química, física e biologia. Na indústria, a computação quântica promete revolucionar processos de otimização, análise de dados e inteligência artificial, oferecendo eficiências inéditas e impulsionando a inovação.

A computação quântica, além de suas aplicações práticas, evidencia a habilidade humana de compreender e manipular os princípios fundamentais do universo. Ela combina teoria e prática ao unir a física quântica com a engenharia de computação, desafiando concepções tradicionais sobre computação e informação.

Os desafios técnicos, como a decoerência quântica, a escalabilidade e o controle de erros, são obstáculos que ainda limitam a aplicação mais ampla dessa tecnologia. No entanto, os avanços recentes em hardware quântico e a busca por criptografia pós-quântica mostram que o desenvolvimento está em pleno andamento.

Em resumo, a computação quântica representa não apenas uma próxima fase na evolução da tecnologia, mas é um salto paradigmático que amplia os limites do que a tecnologia pode realizar. Ao avançarmos na

exploração e no desenvolvimento dessa tecnologia, estamos não só influenciando o futuro da tecnologia, mas também o futuro da sociedade e do conhecimento humano.

Para que a computação quântica evolua, será fundamental investir em pesquisas que aprimorem a correção de erros e a fidelidade dos qubits, além de viabilizar o uso de qubits em sistemas maiores e mais complexos. As conexões entre a computação quântica e áreas como inteligência artificial prometem inovações que poderão redefinir o processamento de dados e a análise de grandes volumes de informação.

Apesar da incerteza sobre o futuro exato da computação quântica, é inegável que seu impacto será significativo, influenciando praticamente todos os setores da tecnologia, ciência e sociedade. Nos próximos anos, a evolução da computação quântica envolverá encontrar um equilíbrio entre explorar seu amplo potencial e lidar com os desafios técnicos, éticos e sociais que surgem com esse avanço tecnológico.

REFERÊNCIAS

AARONSON, S. **Quantum computing since Democritus**. [S.l.]: Cambridge University Press, 2013.

AARONSON, S.; GREEN, F. Review of quantum computing since democritus. **ACM SIGACT News**, v. 44, n. 4, p. 42-47, 2013.

ABDELGABER, N.; NIKOLOPOULOS, C. Overview on quantum computing and its applications in artificial intelligence. *In*: IEEE THIRD INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND KNOWLEDGE ENGINEERING (AIKE). [S.l.], 2020. p. 198-199.

ABUGHANEM, M.; ELEUCH, H. Nisq computers: A path to quantum supremacy. **arXiv preprint arXiv:2310.01431**, 2023.

AGUADO, R.; KOUWENHOVEN, L. P. Majorana qubits for topological quantum computing. **Physics today**, American Institute of Physics, v. 73, n. 6, p. 44-50, 2020.

ARAÚJO-MOREIRA, F. M. *et al.* **Tecnologias quânticas: a inovação disruptiva como diferencial estratégico para a defesa nacional.** [S.l.]: Seven Editora, 2023.

CEREZO, M. *et al.* Challenges and opportunities in quantum machine learning. **Nature Computational Science**, New York, Nature Publishing Group US, v. 2, n. 9, p. 567–576, 2022.

CUOMO, D.; CALEFFI, M.; CACCIAPUOTI, A. S. Towards a distributed quantum computing ecosystem. **IET Quantum Communication**, Wiley Online Library, v. 1, n. 1, p. 3–8, 2020.

DUNJKO, V.; WITTEK, P. A non-review of quantum machine learning: trends and explorations. **Quantum Views**, Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften, v. 4, p. 32, 2020.

FOX, M. F.; ZWICKL, B. M.; LEWANDOWSKI, H. Preparing for the quantum revolution: What is the role of higher education? **Physical Review Physics Education Research**, APS, v. 16, n. 2, p. 201–31, 2020.

GARG, S.; RAMAKRISHNAN, G. Advances in quantum deep learning: An overview. **arXiv preprint arXiv: 2005.04316**, v. 1, may. 2020.

GILL, S. S. *et al.* Quantum computing: A taxonomy, systematic review and future directions. **Software: practice and experience**, Wiley Online Library, v. 52, n. 1, p. 66–114, 2022.

HERMAN, D. *et al.* A survey of quantum computing for finance. **arXiv preprint arXiv:2201.02773**, 2022.

MALIKOVICH, K. M.; TASHEV, K.; SAFOEV, N. Opportunities, challenges, and ethical considerations of quantum computing in technology and business. **Scientific Journal Impact Factor**, v. 2, n. 23, p. 112, dez. 2023.

MCARDLE, S. *et al.* Quantum computational chemistry. **Reviews of Modern Physics**, APS, v. 92, n. 1, p. 015003, 2020.

NITA, L. *et al.* The challenge and opportunities of quantum literacy for future education and transdisciplinary problem-solving. **Research in Science & Technological Education**, Taylor & Francis, v. 41, n. 2, p. 564–580, 2023.

OLLITRAULT, P. J.; MIESSEN, A.; TAVERNELLI, I. Molecular quantum dynamics: A quantum computing perspective. **Accounts of Chemical Research**, ACS Publications, v. 54, n. 23, p. 4229–4238, 2021.

PERRIER, E. Ethical quantum computing: A roadmap. **arXiv preprint arXiv:2102.00759**, 2021.

QUAIS, I.; MOORE, L. D. Editorial (português): uma breve história do hardware, seus desafios, e impacto sobre o consumo de energia. **Academic Journal On Computing, Engineering And Applied Mathematics**, v. 3, n. 2, out., 2022.

RAJAK, A. *et al.* Quantum annealing: An overview. **Philosophical Transactions of the Royal Society A**, The Royal Society, v. 381, n. 2241, p. 20210417, 2023.

RASA, T.; PALMGREN, E.; LAHERTO, A. Futurising science education: students' experiences from a course on futures thinking and quantum computing. **Instructional Science**, Springer, v. 50, n. 3, p. 425–447, 2022.

ROY, T. *et al.* Programmable superconducting processor with native three-qubit gates. **Physical Review Applied**, APS, v. 14, n. 1, p. 014072, 2020.

SAHOO, S. *et al.* A critical overview on quantum computing. **Journal of Quantum Computing**, Tech Science Press, v. 2, n. 4, p. 181, 2020.

SCHULD, M.; KILLORAN, N. Is quantum advantage the right goal for quantum machine learning? **Prx Quantum**, APS, v. 3, n. 3, p. 030101, 2022.

SHARA, J. Quantum machine learning and cybersecurity. **Quantum**, v. 12, n. 6, p. 47–56, 2023.

SIGOV, A.; RATKIN, L.; IVANOV, L. A. Quantum information technology. **Journal of Industrial Information Integration**, Elsevier, v. 28, p. 100365, 2022.

SILVA, M. L. P. da. Tecnologia é atemporal, só precisa ser bem usada. **Rev. Bras. Apl. Vac.**, Campinas, v. 39, n. 1, p. 1-1, jan./mar. 2020.

SMITH, A. *et al.* Crossing a topological phase transition with a quantum computer. **Physical Review Research**, APS, v. 4, n. 2, p. L22020, 2022.

TACCHINO, F. *et al.* Quantum computers as universal quantum simulators: state-of-the-art and perspectives. **Advanced Quantum Technologies**, Wiley Online Library, v. 3, n. 3, p. 1900052, 2020.

VAZQUEZ, M.; PANTAROTTO, G.; BATTILANA, R. Distribuição de chaves criptográficas com o uso do protocolo quântico bb84. *In*: FATECSEG-CONGRESSO DE SEGURANÇA DA INFORMAÇÃO, 2021. [S.l.: s.n.], 2021.

WANG, Y. Quantum computation and quantum information. **Statistical Science**, v. 27, n. 3, p. 373-394, 2012.

WU, Y. *et al.* Strong quantum computational advantage using a superconducting quantum processor. **Physical review letters**, APS, v. 127, n. 18, p. 180501, 2021.

XIN, T. *et al.* Quantum algorithm for solving linear differential equations: Theory and experiment. **Physical Review A**, APS, v. 101, n. 3, p. 032307, 2020.

ZHANG, S. B. *et al.* Topological and holonomic quantum computation based on second-order topological superconductors. **Physical Review Research**, APS, v. 2, n. 4, p. 043025, 2020.

Conflito de interesse

Os autores declaram que não existem conflito de interesses.