



ARTIGO

A REVOLUÇÃO DAS TECNOLOGIAS QUÂNTICAS: CAMINHOS PARA O DESENVOLVIMENTO NACIONAL

POR

Antônio Abelém
abelem@ufpa.br

As tecnologias quânticas emergem como uma das áreas científicas e tecnológicas mais promissoras da atualidade, com impacto potencial em comunicação segura, computação de alto desempenho, novas arquiteturas de redes e sistemas avançados de sensoriamento. Países que estruturarem de forma coordenada e contínua suas capacidades científicas, industriais e regulatórias poderão alcançar protagonismo global e soberania tecnológica em áreas críticas. No Brasil,

apesar do crescimento de grupos de pesquisa e da participação em iniciativas internacionais, persistem desafios estruturais que dificultam o crescimento contínuo e a participação ativa do país nesta nova revolução tecnológica.

Este artigo apresenta uma análise dos desafios e oportunidades do ecossistema quântico brasileiro, com foco em quatro eixos essenciais: hardware quântico; infraestrutura e redes quânticas; cibersegurança e criptografia pós-quântica; e formação de recursos humanos especializados.

Desafios em Hardware, Algoritmos e Software Quântico

O ponto de partida para qualquer ecossistema quântico robusto é o desenvolvimento de hardware nacional. Embora avanços importantes tenham sido feitos globalmente, a construção de bits quânticos, os qubits, funcionais e estáveis continua sendo uma das barreiras mais complexas. Dispositivos quânticos são intrinsecamente sensíveis ao ambiente: ruído térmico, vibrações, instabilidades eletromagnéticas e imperfeições materiais comprometem diretamente a fidelidade das operações.

No caso do Brasil, essa dificuldade é agravada pela dependência de equipamentos importados e pela ausência de linhas de fabricação e caracterização de materiais quânticos em escala. A criação de laboratórios nacionais capazes de produzir componentes como:

- qubits supercondutores,
- fontes de fótons emaranhados,
- ressonadores,
- chips para fotônica integrada,
- repetidores e roteadores quânticos,

seria crucial para reduzir a vulnerabilidade tecnológica e fortalecer a soberania científica. Além de atender às necessidades de pesquisa, essa capacidade fabril permitiria ao país participar de cadeias globais de suprimento em uma área que tende a se tornar estratégica para a indústria de alta tecnologia.

O domínio do hardware é também indispensável para avançar em áreas como computação quântica, comunicação quântica e sensoriamento de precisão, especialmente em aplicações relacionadas à defesa, finanças, metrologia e monitoramento ambiental.

O avanço das tecnologias quânticas também exige o desenvolvimento de algoritmos e ferramentas de software capazes de explorar plenamente as propriedades dos qubits. Criar algoritmos que apresentem vantagem real sobre métodos clássicos requer novas bases conceituais e o uso de simuladores quânticos em máquinas de alto desempenho, etapa fundamental enquanto o hardware ainda é limitado. Além disso, o ecossistema de software quântico, incluindo linguagens, compiladores e frameworks, ainda carece de padronização e maior eficiência. Superar esses desafios é crucial para transformar resultados experimentais em aplicações quânticas práticas e escaláveis.

Infraestrutura e Redes Quânticas

As redes quânticas constituem a espinha dorsal da comunicação quântica e de diversas aplicações emergentes. Elas permitem que estados quânticos sejam transmitidos entre dispositivos distantes, criando possibilidades como:

- distribuição de chaves quânticas (QKD);
- interconexão de computadores

quânticos;

- redes de sensoriamento quântico distribuído;
- experimentos multi-institucionais em larga escala.

Apesar dos recentes avanços na área, ainda não há uma pilha de protocolos madura e integrada para comunicação quântica, o que dificulta a interoperabilidade entre equipamentos e instituições. É necessária uma arquitetura de rede quântica que vá além de demonstrações pontuais e permita sua expansão gradual em nível metropolitano, regional e nacional.

Para isso, são fundamentais:

1. **Protocolos padronizados** que garantam comunicação eficiente entre diferentes dispositivos e plataformas;
2. **Infraestrutura óptica dedicada**, com fibras de baixíssima atenuação e suporte a enlaces híbridos quântico-clássicos;
3. **Sistemas de sincronização e controle** capazes de gerenciar emissões, detecções e medições quânticas em tempo real;
4. **Testbeds nacionais**, nos moldes dos grandes centros internacionais, que permitam experimentação contínua e formação de especialistas.

O Brasil já conta com iniciativas embrionárias, como redes metropolitanas piloto em alguns centros de pesquisa, como Rio de Janeiro, Salvador e Recife, mas ainda falta escala, padroniza-

ção e integração nacional. O desenvolvimento de repetidores quânticos, dispositivos essenciais para permitir comunicação a longas distâncias, é outro ponto crítico e estratégico.

Segurança e Criptografia Pós-Quântica

Um dos pontos mais sensíveis em relação à computação quântica, é o impacto dos computadores quânticos sobre a segurança digital global. Algoritmos criptográficos amplamente utilizados atualmente, como RSA e ECDSA, podem se tornar vulneráveis diante de computadores quânticos suficientemente poderosos. Essa ameaça torna urgente a adoção de criptografia resistente a ataques quânticos.

A transição para a criptografia pós-quântica (PQC) envolve muito mais do que substituir algoritmos. Trata-se de um processo complexo que requer:

- adaptação de sistemas legados;
- testes de interoperabilidade;
- revisão de protocolos de rede;
- mudanças regulatórias;
- formação de especialistas em segurança quântica;
- certificação e normalização de soluções nacionais.

Nesse contexto, é necessário desenvolver algoritmos e implementações nacionais adaptadas às demandas do país, especialmente para sistemas críticos do governo, bancos e setores industriais estratégicos. Além da PQC, a comunicação quântica via QKD tam-

bém desponta como alternativa para aplicações que exigem máxima segurança, embora ainda enfrente desafios de custo, escalabilidade e padronização.

Formação de Recursos Humanos e Ecossistema Nacional

O avanço das tecnologias quânticas depende diretamente da disponibilidade de profissionais altamente qualificados. O desenvolvimento da área, exige competências interdisciplinares, que exige domínio simultâneo em física, computação, engenharia, matemática e materiais avançados.

Atualmente, o Brasil enfrenta limitações importantes para o avanço das tecnologias quânticas. Há poucos cursos de graduação e pós-graduação que ofereçam trilhas específicas em computação ou comunicação quânticas, o que reduz a formação de especialistas na área. Soma-se a isso a falta de laboratórios didáticos e de pesquisa com infraestrutura robusta, elemento essencial para o desenvolvimento de competências práticas e experimentais. Outro desafio é a dificuldade de atrair estudantes para um campo de alta complexidade, que exige forte base interdisciplinar. Além disso, o país ainda carece de programas nacionais de mobilidade, cooperação e capacitação, fundamentais para estimular a troca de conhecimento, a formação continuada e a consolidação de um ecossistema científico mais integrado.

A superação dessa lacuna exige políticas públicas dedicadas, incluindo:

1. **Currículos interdisciplinares** que integrem física quântica aplicada, engenharia quântica e ciência da computação;
2. **Programas de capacitação contínua**, com escolas de verão, hackathons e desafios nacionais;
3. **Parcerias internacionais estruturadas**, incluindo estágios, intercâmbios e projetos multilaterais;
4. **Incentivos à formação de redes de pesquisa**, articulando universidades, institutos de pesquisa e empresas.

Sem esse investimento massivo em capital humano, qualquer avanço em hardware, redes e segurança permanecerá limitado.

Conclusões e Perspectivas

As tecnologias quânticas representam um divisor de águas para o futuro da inovação, segurança digital e competitividade econômica. O Brasil dispõe de competências relevantes, grupos de pesquisa consolidados e potencial científico para ocupar espaço significativo na revolução quântica. Contudo, sem ações coordenadas, especialmente em hardware, redes, PQC e formação de especialistas, o país corre o risco de ampliar sua dependência tecnológica em áreas altamente estratégicas.

Construir um ecossistema quântico nacional é um desafio complexo, que

exige visão de longo prazo, investimentos contínuos e cooperação multissetorial, sendo também uma oportunidade histórica para reposicionar o país na fronteira da ciência e da inovação.

Referências

1. SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Grandes Desafios da Computação no Brasil 2025-2035. Coordenação André Luís de Medeiros Santos e Flávio Rech Wagner. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2025.
2. Nielsen, M.; Chuang, I. Quantum Computation and Quantum Information. Cambridge UP, 2010.
3. NIST. Post-Quantum Cryptography Standardization. 2024.
4. Dowling, J.; Milburn, G. Quantum Technology: The Second Quantum Revolution. 2003.



ANTÔNIO ABELÉM é Professor Titular da Universidade Federal do Pará (UFPA), onde integra o corpo docente do Programa de Pós-Graduação em Computação desde sua criação. Lidera o laboratório de pesquisa em Redes de Computadores e Comunicação Multimídia (GERCOM), conduzindo projetos nacionais e internacionais em redes quânticas, protocolos para Internet Quântica e segurança de redes. Coordenou iniciativas como Protocolos de Roteamento para Internet Quântica e integra projetos estratégicos como EcoSustain, o ICONIOT, Smartness e OpenRAN@Brasil. É o coordenador do Grupo de Interesse de Computação e Comunicação Quânticas (GI-CQ). É Pesquisador de Produtividade do CNPq, membro do conselho da SBC e foi pesquisador visitante em UMASS Amherst (2019-2020). Recebeu em 2024 o prêmio de Pesquisador Destaque do SBRC por suas contribuições científicas e à SBC.