

Desafios Computacionais para uma Internet Quântica Brasileira

Antônio Abelém¹, Alberto Schaeffer-Filho², Gabriel Nazar², Jéferson Nobre²,
Juliano Wickboldt², Lisandro Granville², Luciano Gaspar², Weverton Cordeiro²

¹Universidade Federal do Pará (UFPA)

²Universidade Federal do Rio Grande do Sul (UFRGS)

Resumo. A Computação Quântica tem emergido como uma revolução nas tecnologias computacionais, prometendo resolver problemas complexos, como fatoração de grandes números e desenvolvimento de medicamentos. No entanto, surgem preocupações, como, por exemplo, a vulnerabilidade da criptografia atual a ataques quânticos. Além disso, a Computação Quântica está impulsionando a criação de redes quânticas, com impacto significativo em interconectividade e aplicações distribuídas. No Brasil, há uma demanda crescente por uma evolução da Internet Clássica nacional para sua integração com essas redes, sendo o principal desafio o desenvolvimento de um ecossistema robusto, focado em pesquisa, inovação e formação de talentos. Neste documento, desafios e oportunidades de pesquisa em Computação para o desenvolvimento da Internet Quântica Brasileira são apresentados. Tal desenvolvimento pode posicionar o país como líder regional e um importante ente global em Comunicação Quântica.

Abstract. Quantum Computing has emerged as a revolutionary force in computational technologies, promising to solve complex problems such as large-number factorization and drug development. However, concerns have arisen, for example, the vulnerability of current cryptographic systems to quantum attacks. In addition, Quantum Computing is driving the creation of quantum networks, which are expected to significantly impact interconnectivity and distributed applications. In Brazil, there is a growing demand for the evolution of the national Classical Internet to enable integration with these emerging networks. The main challenge lies in developing a robust ecosystem focused on research, innovation, and talent development. This document presents the key research challenges and opportunities in computing for the development of the Brazilian Quantum Internet. Such endeavor could position the country as a regional leader and a significant global player in Quantum Communication.

1. Introdução

A Computação Quântica e a Comunicação Quântica emergem como campos de pesquisa que estão redefinindo os fundamentos da Computação e das Tecnologias de Comunicação. A Computação Quântica promete uma revolução ao permitir a resolução de problemas que são intratáveis para computadores clássicos, como a fatoração de grandes números (AHMED, 2024) ou o desenvolvimento de novos fármacos (SANTAGATI et al., 2024). Ao mesmo tempo, a Comunicação Quântica oferece a possibilidade de comunicações mais

seguras, baseadas nos princípios do entrelaçamento quântico e da criptografia quântica (e.g., protocolo BB84 (BENNETT; BRASSARD, 2014)). Nos últimos anos, grandes avanços foram feitos tanto na teoria quanto na experimentação dessas tecnologias, como evidenciado por pesquisas publicadas em eventos internacionais de renome, como a *IEEE International Conference on Quantum Computing and Engineering* (QCE) e em periódicos de alto impacto, como o *Nature* e o *Physical Review Letters*.

As diversas vantagens advindas da Computação Quântica são acompanhadas de algumas preocupações. Por exemplo, a possibilidade da utilização de computadores quânticos em ataques a esquemas de criptografia assimétrica (MAVROEIDIS et al., 2018). Apesar de haver novos esquemas criptográficos resistentes à Computação Quântica, o desenvolvimento, a adaptação e a implantação desses esquemas não é uma tarefa trivial (WANG et al., 2022). Além da resistência dos próprios algoritmos criptográficos, também é necessário assegurar as propriedades de segurança do hardware e do software utilizados. Finalmente, ainda há o desenvolvimento de esquemas criptográficos quânticos, os quais precisam também de garantias para que sua utilização seja difundida.

A emergência da Computação Quântica permite que sejam estabelecidas redes que operam com tecnologia quântica, o que traz impactos especialmente para a Internet. Comunicações quânticas já estão sendo implementadas em redes experimentais (e.g., Rede Quântica de Pequim-Shanghai (CHEN et al., 2021)). Tais redes representam um passo significativo para a criação de uma Internet Quântica, incorporando tecnologia quântica na infraestrutura da Internet. Nos últimos anos, pesquisas e experimentos têm se concentrado no desenvolvimento de protocolos para a Internet Quântica (ABELEM; TOWSLEY; VARDOYAN, 2020) (LI et al., 2024).

Os avanços na Computação e Comunicação Quântica não apenas sublinham a importância estratégica dessa área, mas também destacam a necessidade urgente do desenvolvimento de uma Internet Quântica Brasileira. Tal necessidade tem sido reconhecida por instituições científicas e governamentais. A Sociedade Brasileira de Computação (SBC) criou em 2024 o Grupo de Interesse em Computação e Comunicação Quântica (GICQ), e o Ministério da Ciência, Tecnologia e Inovação (MCTI) do Governo Federal criou internamente um Grupo de Trabalho (GT) dedicado às tecnologias quânticas. Ademais, na 5ª Conferência Nacional de Ciência e Tecnologia, realizada em Brasília em 2024, as questões de tecnologias quânticas foram debatidas em uma sessão plenária, refletindo o reconhecimento do tema como uma prioridade estratégica para o futuro do país.

Neste contexto, surge o grande desafio de desenvolver o ecossistema da Internet Quântica Brasileira de forma integrada. Esse ecossistema se faz imprescindível para posicionar o Brasil na vanguarda desta nova era tecnológica. Nesse documento, defendemos que um dos Grandes Desafios a serem superados é a capacidade de desenvolver e utilizar mecanismos e técnicas computacionais com desenvolvimento nacional em conjunto com a formação de talentos e o desenvolvimento de pesquisas de ponta. O fomento a um ambiente acadêmico e inovador possibilitará o estabelecimento de parcerias internacionais e financiamento de projetos inovadores. O esforço dispendido contribuirá para o avanço global da ciência e para o fortalecimento da posição da Brasil como um centro de excelência em Comunicação Quântica.

A presente proposta está descrita como segue. Na Seção 2, será apresentada a fundamentação em relação à Computação Quântica e a Comunicação Quântica. Na Seção 3, serão discutidos os desafios para o estabelecimento da Internet Quântica Brasileira.

2. Fundamentação Teórica

Um sistema quântico é descrito por seu estado quântico, o qual representa uma descrição completa do sistema em um momento específico. O equivalente clássico de um estado quântico seria uma sequência de valores binários. Assim como um bit individual (0, 1), um sistema quântico pode consistir em um único qubit, o qual existe como uma superposição de 2 possibilidades dentro do mesmo espaço binário ($a | 0 \rangle + b | 1 \rangle$). No entanto, como os estados quânticos são regidos pelas leis da mecânica quântica, seu comportamento é significativamente diferente de um bit. Nesta seção, resumiremos alguns conceitos-chave da Computação Quântica. Em seguida, explicaremos suas implicações para as redes quânticas, em especial para a Internet Quântica.

Alguns conceitos da Computação Quântica são particularmente importante para as redes quânticas: emaranhamento, par de Bell, teletransporte, e troca de emaranhamento. O emaranhamento é o bloco de construção fundamental das redes quânticas. Qubits emaranhados têm propriedades não-locais interessantes, as quais podem ser usadas para comunicação. Pares de Bell são um tipo especial de estado quântico, no qual dois qubits exibem emaranhamento máximo. Por meio do teletransporte, a transmissão de um estado quântico desconhecido pode ser realizada. Finalmente, a troca de emaranhamento é o processo de distribuir um emaranhamento entre duas partes distantes por meio de alguns nós intermediários, o que é feito através do compartilhamento de um par de Bell.

A comunicação clássica (i.e., não-quântica) é um elemento fundamental das redes quânticas. As tarefas realizadas nessas redes também necessitam de conectividade clássica. Dentre essas tarefas, pode ser citado o gerenciamento da geração e troca de emaranhamentos. Protocolos distribuídos clássicos de sinalização e controle possibilitam tal gerenciamento. Dessa forma, uma rede quântica possui dois planos de dados, um clássico e um quântico. Além disso, as informações entre esses planos precisam ser correlacionadas (KOZLOWSKI et al., 2023).

A Internet Clássica é uma rede de redes clássicas, as quais podem ser definidas como um conjunto de nós que é capaz de trocar bits através de pacotes. De forma análoga, a Internet Quântica é uma rede de redes quânticas, as quais são definidas como um conjunto de nós que é capaz de trocar qubits e distribuir estados emaranhados entre si. A Internet Quântica será executada em conjunto com a Internet Clássica.

A emergência da Computação Quântica tem propiciado melhorias em aplicações tradicionais e o surgimento de aplicações quânticas. Os computadores quânticos podem ajudar no desenvolvimento de novos materiais e acelerar a descoberta de medicamentos e as decisões tomadas sobre transações financeiras. A Internet Quântica também oferece promessas para diversas novas aplicações (WANG et al., 2024). Este documento foca em aplicações quânticas que têm mais impacto na Internet Quântica, como configuração de comunicação segura e computação quântica distribuída.

3. Desafios, Áreas Habilitadoras e Oportunidades

A área da Computação tem muito a contribuir no desenvolvimento da Internet Quântica Brasileira. O processo de integração da Internet Quântica com a Internet Clássica é semelhante ao processo de introdução de novos paradigmas de comunicação na Internet já existente, mas com impactos mais significativos. A seguir, são discutidos desafios e oportunidades de pesquisa em um conjunto amplo de áreas da Computação.

Infraestrutura Nacional para a Internet Quântica. *Desafio:* Muitas infraestruturas nacionais e regionais têm sido desenvolvidas para a Internet Quântica. Podem ser citados os seguintes exemplos: Pequim-Shanghai (China), Jinan-Qingdao (China), DARPA (EUA), SwissQuantum (Suíça), Tóquio (Japão), entre outras. No Brasil, recentemente foi lançada a Rede Rio Quântica. No entanto, tais redes operam principalmente para experimentos relacionados com criptografia, não necessariamente usando uma pilha de protocolos compatíveis com a Internet (e.g., sem seguir padrões do *Internet Engineering Task Force* - IETF). Além disso, considerando o caso brasileiro, a rede possui abrangência apenas metropolitana. Dessa forma, o desenvolvimento de uma Internet Quântica nacional se impõe como uma desafio.

Desenvolvimento de Hardware e Software para Equipamentos para Internet Quântica. *Desafio:* Diversas necessidades de hardware e software são necessárias para o estabelecimento da Internet Quântica. Em relação à hardware, podem ser mencionados repetidores quânticos (e.g., responsáveis pela troca de emaranhamento) e roteadores quânticos (e.g., responsáveis pelo plano de controle da rede quântica). Já em relação ao software, podem ser mencionadas tanto aplicações especializadas a serem executadas nos nós quânticos finais quanto software de controle específicos para os nós que implementam a infraestrutura da rede. Apesar do hardware e software para redes quânticas ter potencialmente abrangência mundial, seria de grande importância a participação brasileira. Tal participação poderia posicionar o país como um dos líderes nessas redes, além de garantir a soberania quântica nacional. Além disso, no contexto desse desenvolvimento, espera-se o incentivo ao ecossistema de inovação no entorno da Internet Quântica Brasileira (e.g., com o surgimento de startups).

Desenvolvimento de Abordagens para o Gerenciamento e Operação da Internet Quântica *Desafio:* Diversas iniciativas de pesquisa têm sido propostas para concretizar a Internet Quântica (e.g., propondo melhorias em sua tolerância a erros). No entanto, pouco trabalhos enfrentam os desafios computacionais relacionados com abordagens para o gerenciamento e operação de rede até o presente momento. Diversas tarefas relacionadas com essas abordagens serão necessárias, como, por exemplo, descoberta da topologia e serviços da rede, gerenciamento de recursos, etc. Além de protocolos padronizados para o plano de controle de redes quânticas, também serão necessárias melhores práticas que assegurem um funcionamento adequado das Internet Quântica. Esses protocolos podem se utilizar apenas de comunicação clássica ou também necessitar de processos quânticos para sua operação.

Cenários de Transição da Internet Clássica Brasileira para sua Evolução Quântica

Desafio: Durante a transição da Internet Clássica Brasileira para sua evolução quântica são esperados diversos desafios relacionados com tal evolução. Por exemplo, a escolha da utilização de criptografia resistente à computação quântica ou de criptografia quântica pode estar relacionada com requisitos específicos de cibersegurança das aplicações. Além disso, essa escolha também pode estar relacionada com as funcionalidades presentes nos nós participantes de uma determinada tarefa. Os cenários de transição potencialmente necessitam de uma coordenação entre um plano de controle clássico em conjunto com um quântico.

Desenvolvimento de Aplicações relacionadas à Realidade Brasileira para a Internet Quântica

Desafio: A infraestrutura esperada para a Internet Quântica Brasileira pressupõe o suporte a diferentes tipos de aplicações quânticas distribuídas, heterogeneidade em relação a hardware e software, e respeito a padrões internacionais. No entanto, as particularidades da realidade brasileira precisam ser consideradas, especialmente no que tange ao desenvolvimento de aplicações. Dessa forma, espera-se que a comunidade acadêmica participe ativamente no projeto de aplicações com alto impacto nas questões mais significativas para a população brasileira

Referências

ABELEM, A.; TOWSLEY, D.; VARDOYAN, G. Quantum internet: The future of internetworking. In: _____. *Shortcourses' Book of the XXXVIII Brazilian Symposium on Computer Networks and Distributed Systems (SBRC 2020)*. Porto Alegre, RS, Brasil: Brazilian Computing Society SBC, 2020. cap. 2.

AHMED, N. Quantum computing algorithms for integer factorization: A comparative analysis. *Modern Dynamics: Mathematical Progressions*, v. 1, n. 1, p. 6–9, 2024.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, Elsevier, v. 560, p. 7–11, 2014.

CHEN, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, Nature Publishing Group UK London, v. 589, n. 7841, p. 214–219, 2021.

KOZLOWSKI, W. et al. *RFC 9340 Architectural principles for a quantum internet*. Wilmington, DE, USA: RFC Editor, 2023.

LI, Y. et al. A survey of quantum internet protocols from a layered perspective. *IEEE Communications Surveys & Tutorials*, IEEE, 2024.

MAVROEIDIS, V. et al. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, The Science and Information Organization, v. 9, n. 3, 2018. Disponível em: <http://dx.doi.org/10.14569/IJACSA.2018.090354>.

SANTAGATI, R. et al. Challenges and opportunities for applying quantum computers to drug design. *Bulletin of the American Physical Society*, APS, 2024.

WANG, C. et al. *RFC 9583 Application Scenarios for the Quantum Internet*. Wilmington, DE, USA: RFC Editor, 2024.

WANG, J. et al. Quantum-safe cryptography: crossroads of coding theory and cryptography. *Science China Information Sciences*, Springer, v. 65, n. 1, p. 111301, 2022.