INTERNET QUÂNTICA: REALIDADE OU SONHO?

Regina Melo Silveira
Escola Politécnica da Universidade de São Paulo, SP, Brasil

RESUMO

Este trabalho mostra que o uso de tecnologias quânticas já é uma realidade e faz um breve levantamento do desenvolvimento dos sistemas QKD (*Quantum Key Distribution*) e da possibilidade desta tecnologia ser ampliada e servir de base para a Internet Quântica. Uma reflexão sobre os desafios e avanços tecnológicos necessários também é apresentada.

PALAVRAS-CHAVE

Sistemas QKD, Tecnologia Quântica, Internet Quântica

1. INTRODUÇÃO

Nos últimos anos as tecnologias quântica têm evoluído significativamente, viabilizando a utilização de computadores quânticos, sensores quânticos e redes quânticas de propósito específico, conhecidas como Distribuição de Chaves Quânticas (QKD - *Quantum Key Distribution*).

Os computadores quânticos já se encontram disponíveis, através de serviços de nuvem de empresas como IBM[1], Microsoft[2], Google[3] e Rigetti[4]. Estas empresas, além de investir na arquitetura e construção de computadores quânticos, têm também produzido *kits* de desenvolvimento para tais computadores. Estes são compostos por plataforma de desenvolvimento, simuladores, linguagens e bibliotecas, e são colocados à disposição da comunidade de desenvolvedores de software, com licença Apache 2.0 (software livre). Com estes kits, QisKit[5] (IBM), Cirq[6] (Google), Azure Quantum[7] (Microsoft) e Forest[8] (Rigetti), é possível desenvolver algoritmos, testá-los em um simulador e então submetê-los a um computador quântico real, para obter o resultado do processamento (Hidary, 2021). Possivelmente ainda teremos que esperar alguns anos para ter um computador quântico em nosso escritório, pois ainda existem vários desafios a serem superados, como a temperatura de operação, que em algumas arquiteturas é necessário manter o processador a -273 ºC (ou 0ºK), e o número de qubits (quantum bits) disponíveis, que ainda são restrito. A máquina atualmente em operação com maior quantidade de qubits é o Eagle Quantum da IBM com 127 qubits. Mas a IBM já anunciou o lançamento de outro computador quântico de 413 qubits para este ano. Apesar de todos os desafios ainda existentes, já podemos dizer que o Computador Quântico já é uma realidade.

Os sensores quânticos, que são dispositivos que utilizam subpartículas atômicas e suas características, para a detecção de algum processo molecular em um ser vivo, já se encontram em operação em inúmeros exames médicos de imagens. Como exemplo pode-se citar MEG (magnetoencefalografia), ULF-MRI (imagens de ressonância magnética do cérebro em campo ultra-baixo) (Burmistrov et al. 2012), MMG (mamografia) e MCG (magnetocardiograma)(Miyamoto et al. 2008), que são utilizados tanto em humanos como em animais. Além disso, esta tecnologia deve compor o que é chamado de "Próxima Geração de Diagnóstico in vivo", onde técnicas de imagem através de dispositivos implantáveis, utilizando nanoimagem

[1] https://www.ibm.com/quantum/systems
[2] https://azure.microsoft.com/en-us/services/quantum/
[3] https://quantumai.google/
[4] https://www.rigetti.com/
[5] https://github.com/Qiskit
[6] https://github.com/quantumlib/Cirq
[7] https://github.com/Microsoft/Quantum
[8] https://github.com/rigetti/pyquil

ou imagem molecular, que envolvem técnicas para o estudo de eventos moleculares in vivo e também para manipulação de moléculas (Jin et al, 2022). Os principais benefícios da utilização deste tipo de diagnósticos são a detecção precoce de doenças e o monitoramento dos estágios da doença, levando à medicina individualizada e à avaliação em tempo real da eficácia terapêutica e cirúrgica (Mali, S. 2013). Estes sensores, de alta sensibilidade, também devem trazer contribuições significativas como ferramentas para localização de tecidos e estruturas em cirurgias. Apesar de parecer ser a utilização de maior impacto, outros usos, além da área da saúde, também são previstos para os sensores quânticos, principalmente por serem sensores de pequena dimensão e de grande precisão (Villatoro, J., 2020).

Com relação a tecnologia QKD, há alguns anos já são uma realidade, em operação inicialmente em laboratórios de pesquisa e rede de testes (*testbeds*), metropolitanas e de longa distância, como é o caso das redes DARPA (Elliot et al., 2005)(Elliot, C., 2018), SECOQC (Peev et al., 2009), Cambridge (Dynes et al., 2019), SwissQuantum (Struck et al., 2011) e Beijing-Shanghai (Wang et al., 2017), demonstrando bom desempenho para a distribuição de chaves para estabelecimento de comunicação segura, ou seja, chaves criptográficas. E mais recentemente, já estão em operação em serviços comerciais oferecidos pelas empresas XChange[9]; Toshiba[10]; Quantropi[11], IdQuantique[12], fornecendo serviço de transmissão de chaves criptográficas para instituições financeiras entre outras. Estas redes são envisionadas como as predecessoras da Internet Quântica.

No entanto, existem vários desafios que devem ser superados para que tal rede possa ganhar escalabilidade e possa ser de uso geral, permitindo a transmissão de dados e acesso a serviços que possam se beneficiar com este tipo de conexão. Neste artigo é feito um levantamento dos avanços nas pesquisas e dos desafios a serem ainda superados, para trazer à tona o questionamento das possibilidades de que a Internet Quântica torne-se uma realidade a médio ou longo prazo.

2. QKD

Como mencionado, os sistemas de Distribuição de Chaves Quânticas (QKD) são utilizados para transmitir chaves criptográficas, utilizando para tanto três propriedades quânticas, descritas a seguir:

– Superposição - estado de um qubit em que ele oscila entre seus valores de polarização, podendo assumir diversos valores, permitindo ganhos exponenciais na representação da informação (Hidary, J.D., 2021);

– Emaranhamento ou entrelaçamento - propriedade que permite que dois elementos subatômicos de dois átomos distintos, ou seja, um par de qubits, seja colocado em um estado quântico tal que os permita interagir de forma a terem sempre polaridades opostas. Depois de entrarem em estado de emaranhamento, essa propriedade pode persistir mesmo se esses elementos forem mantidos distantes um do outro;

– Não cópia - essa propriedade se dá devido à alta suscetibilidade a interferências, e a instabilidade de qubits em superposição e em emaranhamento. Assim sendo, qualquer interferência que haja, faz com que os qubits sofram uma decoerência quântica, ao sofrer um decaimento e perdendo a informação que estava representada nele. Sendo assim, pode-se dizer que os qubits não são sujeitos a cópia (Piqueira, J., 2011).

A característica de não cópia garante a segurança da informação transmitida, permitindo que informações vulneráveis, como é o caso das chaves criptográficas, sejam transmitidas sem risco, como mostra a figura 1. Sendo assim, o sistema que utiliza troca de qubits emaranhados é utilizado para a comunicação entre duas entidades, representados por Alice e Bob na figura, em que trocam a chave criptográfica, através de um canal quântico. Bob, ao receber a chave verifica se a chave está intacta, e trocam a informação criptografada por esta chave pelo canal clássico. Caso a chave recebida não esteja intacta, Bob solicita uma nova chave a Alice pelo canal clássico, até que a chave esteja adequada, representando que o processo está seguro, e aí são enviados os dados criptografados com esta chave.

Os sistemas QKD experimentais e comerciais mencionados anteriormente têm sido implantados utilizando fibras ópticas ou links de satélite. No entanto, os sistemas que utilizam fibra óptica, com

[9] https://quantumxc.com/phio/
[10] https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html
[11] https://www.quantropi.com/
[12] https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/

transmissão baseada em WDM (*Wavelength-Division Multiplexing*), têm se mostrado mais estável, mais maduro e de menor custo em comparação ao implementado com enlace de satélite. Os sistemas QKD baseados em transmissão por fibra óptica ainda podem se beneficiar da utilização de dispositivos ópticos já disponíveis no mercado, utilizados pelas redes WDM. No entanto, a expectativa é que os dois modos de implantação sejam complementares, principalmente porque o enlace de satélite permite cobertura a maiores distâncias (~1200 km contra ~600km na fibra óptica), possibilitando a implantação de redes mais amplas (Cao et al., 2022).

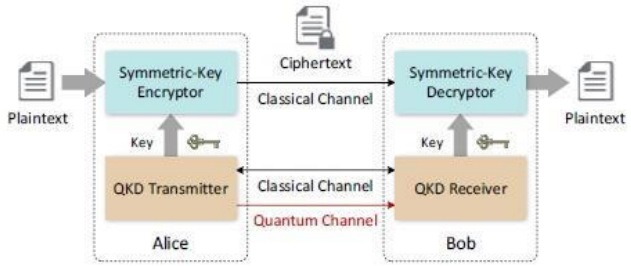

Figura 1. Representação da troca de mensagens no sistema QKD (extraído de Cao et al., 2022)

Diversos protocolos foram desenvolvidos para que possa ser estabelecida a comunicação entre os pares, sendo que na prática os mais utilizados são o BB84 e o COW (Nurhadi, A. I., & Syambas, N. R., 2018). Basicamente eles têm como tarefa fazer a preparação do par de qubit, criando o emaranhamento, a transmissão de um deles e a medida do qubit no destino. Ainda como parte do protocolo de comunicação deve ser feita a verificação da taxa de erro de qubit (QBER), e na fase de pós-processamento, a correção de erro e recuperação da informação original, e finalmente a autenticação, indicando que a informação não está corrompida.

3. EVOLUÇÃO TECNOLÓGICA PARA INTERNET QUÂNTICA

Atualmente o uso comercial de QKD tem mostrado eficiência para conexões par-a-par. A Toshiba, por exemplo, oferece um serviço de transmissão de chaves utilizando protocolo BB84, com modulação a 1GHz, capacidade de 1Mbps, utilizando comprimento de onda de 1550 nm e com probabilidade de perda de 5%. Esta configuração deve ser planejada minuciosamente, já que a taxa de modulação, a taxa de erro de qubit (QBER) e a probabilidade de falha são parâmetros muito sensíveis e necessitam ser adequadamente definidos (Cao et al., 2022).

No entanto, para viabilizar a Internet Quântica será necessário solucionar alguns pontos críticos:

– Ampliar sua capacidade, de forma que passe a ser uma rede multiusuários: os sistemas QKD são restritos a conexões par-a-par, não permitindo simultaneidade devido a incapacidade de gerenciar linhas cruzadas;

– Desenvolver tecnologia para repetidores e amplificadores quânticos: os sistemas QKD atuais utilizam repetidores digitais, sendo necessário fazer a conversão quântico-digital-quântico, criando pontos de vulnerabilidade da rede. No entanto, alguns trabalhos, como o de Ruihong, Q., & Ying, M (2019) apontam para as evoluções para um repetidor totalmente quântico;

– Melhorar mecanismos de correção de erro: os sistemas quânticos atuais ainda são muito sensíveis a interferências e os mecanismos de correção de erros ainda não estão maduros o suficiente para atender a sistemas distribuídos em rede.

Alguns pesquisadores indicam a necessidade de muito investimento para chegarmos a maturidade desta tecnologia, como salientam Wehner, Elkouss e Hanson (2018) que definiram diferentes estágios de desenvolvimento para chegarmos a Internet Quântica completa. Tais estágios de desenvolvimento envolvem tanto *hardware*, como protocolos e *software*, incluindo memória quântica, gerenciamento de processos e melhor desempenho para recuperação de erros e falhas. Por outro lado, vários processos poderão ser desenvolvidos em *software*, trazendo grandes oportunidades e desafios nesta área.

4. CONSIDERAÇÕES FINAIS

A Internet Quântica trará vários benefícios. Além da possibilidade de implementar uma rede segura, como já ocorre com a QKD, existem outras oportunidades com a disponibilidade ampla desta infraestrutura. A computação distribuída possibilitará a ampliação do uso de computadores quânticos com recursos restritos, de tal forma que um algoritmo distribuído possa ser executado por computadores quânticos conectados em rede, formando uma computação quântica federada.

Com a disponibilidade mais ampla da Internet Quântica, aplicações de tempo real e sensíveis a atrasos conseguirão grandes benefícios, já que os qubits emaranhados podem ser manipulados com atrasos muito menores do que as redes atuais, considerados instantâneos.

Ainda há necessidade de muitos desenvolvimentos tecnológicos para a maturidade de uma Internet quântica. Mas os avanços estão acontecendo rapidamente à medida que aumentam os investimentos, principalmente oriundos de países como Estados Unidos da América, China e Japão. Tudo indica que a médio prazo a Internet Quântica será uma realidade e mudará nossa percepção de comunicação em rede.

REFERÊNCIAS

Burmistrov, E., Matlashov, A., Sandin, H., Schultz, L., Volegov, P., & Espy, M. (2012). Optimization and configuration of SQUID sensor arrays for a MEG-MRI system. IEEE transactions on applied superconductivity, 23(3), 1601304-1601304.

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials, 24(2), 839-894.

Dynes, J. F., Wonfor, A., Tam, W. S., Sharpe, A. W., Takahashi, R., Lucamarini, M., ... & Shields, A. J. (2019). Cambridge quantum network. npj Quantum Information, 5(1), 1-8.

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., & Yeh, H. (2005, May). Current status of the DARPA quantum network. In Quantum Information and computation III (Vol. 5815, pp. 138-149). SPIE.

Elliott, C. (2018). The DARPA quantum network. In Quantum Communications and cryptography (pp. 91-110). CRC Press.

Hidary, J. D., & Hidary, J. D. (2021). Quantum computing: an applied approach (Vol. 1). Springer.

Jin, W., Yang, Q., Liu, S., Dong, C., & Ren, T. L. (2022). Sensor-Assisted Next-Generation Diagnostics: Emerging Concepts, Biomarkers, Technologies, and Challenges. Miniaturized Biosensing Devices, 1-37.

Johnston, E. R., Harrigan, N., & Gimeno-Segovia, M. (2019). Programming Quantum Computers: essential algorithms and code samples. O'Reilly Media.

Mali, S. (2013). Nanomedicine–next generation technology revolutionizing medical practice. Journal of Maxillofacial and Oral Surgery, 12(1), 1-2.

Miyamoto, M., Kawai, J., Adachi, Y., Haruta, Y., Komamura, K., & Uehara, G. (2008, February). Development of an MCG/MEG system for small animals and its noise reduction method. In Journal of Physics: Conference Series (Vol. 97, No. 1, p. 012258). IOP Publishing.

Nurhadi, A. I., & Syambas, N. R. (2018, July). Quantum key distribution (QKD) protocols: A survey. In 2018 4th International Conference on Wireless and Telematics (ICWT) (pp. 1-5). IEEE.

Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., ... & Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. New Journal of Physics, 11(7), 075001.

Piqueira, J. R. C. (2011). Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e teletransporte. Revista Brasileira de Ensino de Física, 33.

Ruihong, Q., & Ying, M. (2019, June). Research progress of quantum repeaters. In Journal of Physics: Conference Series (Vol. 1237, No. 5, p. 052032). IOP Publishing.

Stucki, D., Legre, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., ... & Zbinden, H. (2011). Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics, 13(12), 123001.

Villatoro, J. (2020). Grand challenges in physical sensors. Frontiers in Sensors, 1, 1.

Wang, L. J., Zou, K. H., Sun, W., Mao, Y., Zhu, Y. X., Yin, H. L., ... & Pan, J. W. (2017). Long-distance copropagation of quantum key distribution and terabit classical optical data channels. Physical Review A, 95(1), 012301.

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.