O IMPACTO DA COMPUTAÇÃO QUÂNTICA NA ANÁLISE DE DADOS E CIBERSEGURANÇA

THE IMPACT OF QUANTUM COMPUTING ON DATA ANALYSIS AND CYBERSECURITY

Kauan Marques da Luz[1]

Ilma Rodrigues de Souza Fausto[2]

RESUMO EXPANDIDO

A computação quântica representa uma mudança de paradigma ao aplicar princípios da mecânica quântica, como superposição e emaranhamento, para resolver problemas intratáveis pela computação clássica. Este trabalho tem como objetivo analisar os impactos dessa tecnologia na análise de dados e na cibersegurança, destacando desafios, oportunidades e implicações práticas. A metodologia adotada baseou-se em revisão bibliográfica de obras seminais e artigos recentes, abordando fundamentos teóricos, algoritmos quânticos e desafios práticos. No desenvolvimento, discute-se como o Quantum Machine Learning pode acelerar tarefas de otimização e classificação, superando limitações impostas pelo Big Data, e como algoritmos como o de Shor ameaçam a criptografia de chave pública, exigindo soluções como Criptografia Pós-Quântica e Distribuição de Chaves Quânticas. Considera-se que, embora a era NISQ imponha restrições de hardware e software, os avanços indicam que a computação quântica redefinirá os limites do que é computável, impactando diretamente ciência, indústria e segurança digital. Além disso, exploramos os fundamentos da computação quântica, como qubits, superposição e emaranhamento, que permitem paralelismo massivo e correlações não-locais, oferecendo vantagens computacionais inéditas. A análise de dados, tradicionalmente baseada em modelos clássicos, enfrenta desafios crescentes com o Big Data, exigindo novas abordagens para lidar com volume, velocidade e variedade. Nesse contexto, algoritmos quânticos como HHL e VQE surgem como soluções promissoras para problemas de otimização e simulação molecular, enquanto o QML promete acelerar tarefas de aprendizado em espaços de alta dimensão. No campo da cibersegurança, a computação quântica traz uma dualidade: ao mesmo tempo que potencializa a análise de dados, ameaça os sistemas de segurança atuais. O Algoritmo de Shor compromete a criptografia RSA, exigindo novas estratégias como PQC e QKD. A PQC busca desenvolver algoritmos resistentes a ataques quânticos, enquanto a QKD utiliza princípios quânticos para garantir a troca segura de chaves, embora enfrente desafios práticos. Conclui-se que a computação quântica não é apenas uma evolução tecnológica, mas um novo paradigma que transformará a análise de dados e a segurança da informação. Para profissionais e estudantes, compreender seus fundamentos e implicações é essencial

[1] Acadêmico do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email marques.l@estudante.ifro.edu.br

[2] Orientadora, Professora EBTT em Regime de Dedicação Exclusiva no Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO - Orientadora, Doutora, *e-mail*: ilma.rodrigues@ifro.edu.br.

para preparar-se para um futuro onde os limites computacionais serão radicalmente expandidos. Este estudo também discute os desafios técnicos, como decoerência e ruído, que limitam a escalabilidade dos sistemas quânticos, e apresenta perspectivas para superar essas barreiras por meio de algoritmos híbridos e técnicas de correção de erros. A era NISQ, caracterizada por máquinas imperfeitas, exige soluções inovadoras que combinem recursos clássicos e quânticos para extrair valor prático. A revisão da literatura indica que, embora a implementação em larga escala ainda seja um objetivo distante, os avanços recentes em hardware e software apontam para um futuro promissor. Esta pesquisa contribui para a compreensão das implicações da computação quântica, oferecendo uma visão abrangente sobre seu impacto na análise de dados e na cibersegurança, bem como sobre as estratégias necessárias para mitigar riscos e aproveitar oportunidades.

Palavras-chave: Computação quântica; Análise de dados; Machine Learning Quântico; Cibersegurança; Criptografia Pós-Quântica.

Abstract:
Quantum computing represents a paradigm shift by applying principles of quantum mechanics, such as superposition and entanglement, to solve problems intractable by classical computing. This work aims to analyze the impacts of this technology on data analysis and cybersecurity, highlighting challenges, opportunities, and practical implications. The methodology was based on a literature review of seminal works and recent articles, addressing theoretical foundations, quantum algorithms, and practical challenges. The development discusses how Quantum Machine Learning can accelerate optimization and classification tasks, overcoming limitations imposed by Big Data, and how algorithms such as Shor's threaten public-key cryptography, requiring solutions such as Post-Quantum Cryptography and Quantum Key Distribution. It is considered that, although the NISQ era imposes hardware and software restrictions, advances indicate that quantum computing will redefine the limits of what is computable, directly impacting science, industry, and digital security. Furthermore, we explore the fundamentals of quantum computing, such as qubits, superposition, and entanglement, which enable massive parallelism and non-local correlations, offering unprecedented computational advantages. Data analysis, traditionally based on classical models, faces increasing challenges with Big Data, requiring new approaches to handle volume, velocity, and variety. In this context, quantum algorithms such as HHL and VQE emerge as promising solutions for optimization and molecular simulation problems, while QML promises to accelerate learning tasks in high-dimensional spaces. In the field of cybersecurity, quantum computing brings a duality: while enhancing data analysis, it threatens current security systems. Shor's algorithm compromises RSA encryption, requiring new strategies such as PQC and QKD. PQC seeks to develop algorithms resistant to quantum attacks, while QKD uses quantum principles to ensure secure key exchange, although it faces practical challenges. It is concluded that quantum computing is not just a technological evolution but a new paradigm that will transform data analysis and information security. For professionals and students, understanding its fundamentals and implications is essential to prepare for a future where computational limits will be radically expanded. This study also discusses technical challenges, such as decoherence and noise, which limit the scalability of quantum systems, and presents perspectives to overcome these barriers through hybrid algorithms and error correction techniques. The NISQ era, characterized by imperfect machines, requires innovative solutions that combine classical and quantum resources to extract practical value. This research contributes to understanding the implications of quantum computing, providing a comprehensive overview of its impact on data

analytics and cybersecurity, as well as the strategies required to mitigate risks and leverage emerging opportunities.

Keywords: Quantum computing; Data analysis; Quantum Machine Learning; Cybersecurity; Post-Quantum Cryptography.

REFERÊNCIAS

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *In*: PROCEEDINGS of the IEEE International Conference on Computers, Systems and Signal Processing. [S.l.]: IEEE, 1984. p. 175-179.

BIAMONTE, J. et al. Quantum machine learning. **Nature**, v. 549, n. 7671, p. 195-202, 2017.

DAVENPORT, T. H.; HARRIS, J. G. **Competing on Analytics**: The New Science of Winning. Boston: Harvard Business School Press, 2007.

DEUTSCH, D. Quantum theory, the Church–Turing principle and the universal quantum computer. **Proceedings of the Royal Society of London A**, v. 400, n. 1818, p. 97-117, 1985.

EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?. **Physical Review**, v. 47, n. 10, p. 777–780, 1935.

FEYNMAN, R. P. Simulating physics with computers. **International Journal of Theoretical Physics**, v. 21, n. 6/7, p. 467-488, 1982.

GANTZ, J.; REINSEL, D. **The Digital Universe of Opportunities**: Rich Data and the Increasing Value of the Internet of Things. Framingham: IDC, 2014. Disponível em: https://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities.htm. Acesso em: 20 out. 2025.

GARTNER. **Gartner's Analytic Ascendancy Model**. Stamford: Gartner, 2012. Disponível em: https://blogs.gartner.com/it-glossary/gartner-analytic-ascendancy-model/. Acesso em: 21 out. 2025.

HARROW, A. W.; HASSIDIM, A.; LLOYD, S. Quantum algorithm for linear systems of equations. **Physical Review Letters**, v. 103, n. 15, p. 150502, 2009.

INMON, W. H. **Building the Data Warehouse**. 4. ed. Indianapolis: Wiley Publishing, 2005.

KAKU, M. **A Física do Futuro**: como a ciência moldará o destino humano e nossas vidas cotidianas no século XXI. Rio de Janeiro: Rocco, 2012.

KIMBALL, R.; ROSS, M. **The Data Warehouse Toolkit**: The Definitive Guide to Dimensional Modeling. 3. ed. Indianapolis: Wiley, 2013.

LANEY, D. 3D Data Management: Controlling Data Volume, Velocity, and Variety. **Gartner**, 6 fev. 2001. Disponível em: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Acesso em: 21 out. 2025.

MOORE, G. E. Cramming more components onto integrated circuits. **Electronics**, v. 38, n. 8, p. 114-117, 19 abr. 1965.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Post-Quantum Cryptography Standardization**. Gaithersburg: NIST, 2024. Disponível em: https://csrc.nist.gov/Projects/post-quantum-cryptography. Acesso em: 21 out. 2025.

NATIONAL SECURITY AGENCY (NSA). **Quantum Key Distribution (QKD) and Quantum Cryptography (QC)**. Fort Meade: NSA Cybersecurity, 5 jan. 2024. Disponível em: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. Acesso em: 21 out. 2025.

NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. 10. ed. Cambridge: Cambridge University Press, 2010.

PERUZZO, A. et al. A variational eigenvalue solver on a photonic quantum processor. **Nature Communications**, v. 5, p. 4213, 2014.

PRESKILL, J. Quantum Computing in the NISQ era and beyond. **Quantum**, v. 2, p. 79, 2018.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, v. 21, n. 2, p. 120-126, 1978.

SCHRÖDINGER, E. Discussion of probability relations between separated systems. **Proceedings of the Cambridge Philosophical Society**, v. 31, n. 4, p. 555-563, 1935.

SHARDA, R.; DELEN, D.; TURBAN, E. **Business Intelligence, Analytics, and Data Science**: A Managerial Perspective. 4. ed. Boston: Pearson, 2014.

SHOR, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. **SIAM Journal on Computing**, v. 26, n. 5, p. 1484-1509, 1997.