SUPREMACIA QUÂNTICA E CRIPTOGRAFIA

*Erick Galvão da Silva, Leonardo Rodrigues Ribeiro, Stheffani Gonçalves Rocha Emboava, Mariana Godoy Vazquez Miano*

*Faculdade de Tecnologia de Americana*

[*erick.silva82@fatec.sp.gov.br*](mailto:erick.silva82@fatec.sp.gov.br)*,* [*mariana.miano@fatec.sp.gov.br*](mailto:mariana.miano@fatec.sp.gov.br)

***1. Introdução***

A computação quântica é uma área revolucionária com potencial para transformar a forma como processamos e armazenamos informações, resolvendo problemas complexos de maneira mais eficiente que os computadores clássicos. No entanto, seu avanço ameaça à segurança da criptografia convencional, que se torna vulnerável a ataques quânticos.

O artigo apresenta pesquisas técnicas e aplicações práticas para identificar desafios na migração da computação clássica para a quântica, utilizando ambientes quânticos como o Q# da Microsoft em combinação com linguagens clássicas como o Python para explorar o impacto na segurança da criptografia em um banco de dados relacional. A pesquisa incluiu a implementação de bibliotecas e métodos de criptografia em um código e uma análise comparativa dos resultados entre processos quânticos e clássicos.

***2. Metodologia e Materiais***

Para a construção deste trabalho, o principal elemento quântico foi o Algoritmo de Shor, um algoritmo quântico capaz de fatorar números extensos em uma velocidade exponencialmente maior do que em um computador clássico, ameaçando, portanto, métodos criptográficos baseados em grandes números primos, tal como o RSA.

Tendo em vista a demonstração de tal capacidade, o projeto contou com o desenvolvimento de um código na linguagem quântica Q#, processado por um Quantum Workspace dentro do simulador Azure Quantum, para então realizar comparação do tempo de execução com um código de fatoração clássico. Foram utilizadas, além de Q#, as linguagens clássicas Python e SQL para compor os códigos utilizados para medições de tempo.

Python e QSharp são duas linguagens de programação com características distintas e aplicações diversas. Python é uma linguagem popular, que facilita a escrita de códigos limpos e rápidos, com tipagem dinâmica e flexibilidade. QSharp é uma linguagem inovadora, que permite o desenvolvimento de algoritmos quânticos, com abstração de hardware e integração com computação clássica. Ambas as linguagens são relevantes para o avanço da ciência e da tecnologia.

***4. Resultados***

O estudo apresenta uma análise abrangente sobre a interseção entre a computação clássica e quântica, com foco na segurança da criptografia. A computação quântica emerge revolucionariamente, sendo capaz de resolver problemas complexos eficientemente, mas traz consigo um desafio crítico para a segurança da informação devido à capacidade de quebrar algoritmos criptográficos convencionais de forma exponencialmente mais rápida do que os métodos clássicos.

A integração das linguagens Python e SQL adicionou uma dimensão pragmática ao estudo. Python, através de sua clareza e flexibilidade, permitiu o desenvolvimento de códigos e manipulação de informações complexas. A linguagem Q# trouxe a especificidade necessária para a programação quântica, destacando-se como uma ferramenta poderosa para o desenvolvimento de algoritmos quânticos.

O algoritmo de Shor revelou sua superioridade sobre os métodos clássicos de fatoração, enfatizando a capacidade da computação quântica de desafiar paradigmas tradicionais. A velocidade exponencial de execução da computação quântica em comparação com a computação clássica expõe a urgência de desenvolver estratégias de criptografia resistentes a ataques quânticos, e prova que a proteção de dados na era quântica exigirá soluções inovadoras, à medida que os métodos convencionais de criptografia ficam ultrapassados.

***4. Conclusões***

Uma análise comparativa entre os algoritmos quânticos e clássicos para a quebra de dados revela que a computação quântica possui uma eficiência notavelmente superior. Ela é capaz de realizar a quebra de chaves criptografadas de forma exponencialmente mais rápida do que os algoritmos clássicos, o que evidencia a urgência de desenvolver métodos criptográficos quântico-resistentes e implementar medidas robustas para a proteção de dados na era quântica.

***5. Referências***

[1] J. Preskill, Quantum Computing in the NISQ era and beyond, Quantum, 2018.

[2] M. Mosca, D. Stebila, Post-quantum cryptography, Nature, 2018.

[3] M. G. V. Miano, Aplicação de protocolos quânticos e algoritmo de Shor para a Segurança da Informação, Revista Tecnológica da Fatec Americana, 2020.

[4] I. Chuang, M. Nielsen, Quantum Computation and Quantum Information, Cambridge University Press, 2010.

[5] L. Lacava, M. G. V. Miano, Implementação do algoritmo quântico Deutsch-Jozsa em linguagem funcional e no simulador IBM Q Experience, Revista Tecnológica da Fatec Americana, 2018.

[6] M. G. V. Miano, A. S. Oliveira, Desempenho de algoritmos quânticos e clássicos em treinamento de Machine Learning supervisionado, Revista Tecnológica da Fatec Americana, 2022.