CRIPTOGRAFIA: EXPLORANDO A FATORAÇÃO DE NÚMEROS PRIMOS COM ALGORITMO QUÂNTICO

*Erick Galvão da Silva1, Leonardo Rodrigues Ribeiro2, Stheffani Gonçalves Rocha Emboava3, Mariana Godoy Vazquez Miano4*

*1, 2, 3, 4Faculdade de Tecnologia de Americana*

[*erick.silva82@fatec.sp.gov.br*](mailto:erick.silva82@fatec.sp.gov.br)*1,* [*mariana.miano@fatec.sp.gov.br2*](mailto:mariana.miano@fatec.sp.gov.br2)

***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 os desafios na migração da computação clássica para a quântica, utilizando ambientes quânticos como o Azure Quantum da Microsoft, juntamente com linguagens clássicas para explorar o impacto na integridade de um sistema criptográfico. A pesquisa inclui 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, aplicando o algoritmo de Shor, além da linguagem clássica Python, que facilita a manipulação e coleta de dados.

***3. Resultados***

O estudo apresenta uma análise sobre a disparidade entre a computação clássica e quântica, utilizando como principal objeto experimental, a criptografia. Sabendo que a fatoração de grandes números primos é o problema computacional em questão, foi utilizado um código simples e genérico de fatoração em Python. No gráfico temos a quantidade de algarismos de um número, o tempo de execução do código de fatoração, bem como se ele é classificado como primo ou não primo.

Existe uma grande diferença de tempo entre números primos e não primos a partir de X algarismos. Isso se dá pois, no processo de fatoração, o código busca um número primo P pelo qual é possível realizar a fatoração de N. Quando N não é primo, é muito mais fácil para o computador encontrar seus fatores P, contudo, quando N é primo, o código continuará buscando o único fator possível pelo qual é possível fatorar N: ele mesmo. Por isso, quanto maior for N, mais tempo levará para encontrar P, pois nesse caso P = N.

Gráfico, Linha do tempo

Descrição gerada automaticamenteFigura 1 - Gráfico comparativo da fatoração entre números primos e não primos usando Python

*Fonte: Autores*

Figura 2 – Gráfico comparativo da fatoração entre números primos e não primos usando Q#

(Gráfico e texto serão inseridos depois.)

***4. Conclusões***

Observando a análise comparativa dos resultados, provenientes dos códigos clássicos e quânticos de fatoração, conclui-se que a computação quântica possui uma eficiência notavelmente superior, com alto potencial para realizar a quebra de chaves criptográficas.

Contudo, a aplicação de tais algoritmos na prática ainda é um desafio, pois os recursos computacionais quânticos mais robustos possuem custo extremamente elevado, e as principais linguagens quânticas, inclusive Q#, sofrem atualizações frequentemente, dificultando assim a construção de códigos completamente funcionais que possam ser usados amplamente.

***5. Referências***

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

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

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

[4] 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.