**FATORAÇÃO COM ALGORITMO DE SHOR: COMPARAÇÃO ENTRE ABORDAGENS CLÁSSICAS E QUÂNTICAS**

*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 tem o potencial de transformar a maneira como lidamos com informações complexas, superando os limites dos computadores tradicionais. [1] No entanto, essa evolução também ameaça a segurança da criptografia convencional, devido a possíveis ataques quânticos. [2]

Neste artigo, são desenvolvidas pesquisas técnicas e aplicações práticas, com o objetivo de entender os desafios da transição da computação clássica para a quântica. Para tal, utilizou-se o ambiente do Azure Quantum da Microsoft e a linguagem convencional Python, explorando a quebra da integridade da criptografia RSA por meio do algoritmo de Shor.

***2. Metodologia e Materiais***

Para este trabalho, o principal elemento desenvolvido foi o Algoritmo de Shor, [3][4] um algoritmo quântico capaz de fatorar números primos com mais de 15 dígitos em tempo exponencialmente menor do que um computador clássico, ameaçando, portanto, métodos criptográficos baseados em fatores primos extensos, tal como o RSA. [5]

Visando essa demonstração, 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, para a manipulação e coleta de dados.

***3. Resultados***

Inicialmente, é necessário compreender a problemática dos números primos, utilizando exemplares de menor valor para tornar o estudo viável.

Tabela I – Tempo de fatoração de primos e não primos utilizando ferramenta e código clássico.

|  |  |  |
| --- | --- | --- |
| Quantidade de dígitos | Primos | Não primos |
| 6 | 0.189s | 0.001s |
| 7 | 0.739s | 0.005s |
| 8 | 6.826s | 0.441s |
| 9 | 268.915s | 1.505s |
| 10 | 2461.473s | 29.165s |

Encontrar os fatores de P é mais simples quando N não é primo, visto que, se N for primo, o código persiste na busca do único fator possível: o próprio N. Assim, quanto maior o valor de N, maior o tempo necessário para localizar P, pois P = N, tornando dessa maneira, inviável a fatoração de números primos com mais de 15 dígitos em um computador clássico. Agora, observe o mesmo processo, mas executado por linguagens e ferramentas quânticas.

Tabela II – Tempo de fatoração de primos e não primos utilizando algoritmo de Shor

|  |  |  |
| --- | --- | --- |
| Quantidade de dígitos | Primos | Não primos |
| 6 | 0.0003s | 0.0001s |
| 7 | 0.0004s | 0.0240s |
| 8 | 0.0001s | 0.0515s |
| 9 | 0.0001s | 0.0497s |
| 10 | 0.0001s | 0.0325s |

Conforme a Tabela II, podemos observar que o algoritmo quântico é muito mais eficiente para encontrar os fatores de N, seja ele um número primo ou não, pois o tempo de execução do processo mostrou-se exponencialmente menor.

***4. Conclusões***

Considerando os resultados apresentados, é evidente que a computação quântica possui uma eficiência notavelmente superior, e que possui um 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#, estão ainda em desenvolvimento e sofrem constantes alterações, o que acaba inviabilizando a aplicação prática e estável do algoritmo com os recursos disponíveis atualmente.

***5. Referências***

[1] J. Preskill. Quantum Computing in the NISQ era and beyond. Quantum, 2, 79. 2018.

[2] M. Mosca, D. Stebila. Post-quantum cryptography. Nature, 555 (7697), 588-589. 2018.

[3] M. Miano. Aplicação de protocolos quânticos e algoritmo de Shor para a SI. R. T. Fatec Americana, vol. 8 n. 01, 2020.

[4] M. Miano, A. Oliveira. Desempenho de algoritmos quânticos e clássicos em treinamento de ML supervisionado. R. T. Fatec Americana, v. 9 n. 02. 2021.

[5] M. Nielsen, I. Chuang. Quantum Computation and Quantum Information. 10th. Cambridge University Press, p. 1–161. 2010.