**FATORAÇÃO COM ALGORITMO DE SHOR USANDO ABORDAGENS CLÁSSICA E QUÂNTICA**

*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.br4*](mailto:mariana.miano@fatec.sp.gov.br4)

***1. Introdução***

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

A fatoração, processo de decomposição de um número em fatores primos, faz parte de um processo fundamental na criação de chaves criptográficas assimétricas, a criptografia mais comum a ser encontrada em sistemas seguros de computador atualmente.

Neste trabalho desenvolveram-se pesquisas técnicas e aplicações práticas, utilizando o ambiente Azure Quantum da Microsoft, a linguagem multiparadigma Python e a linguagem quântica Q#, com o objetivo de comparar o desempenho entre as abordagens clássica e quântica, quanto à quebra da integridade da criptografia assimétrica.

***2. Metodologia e Materiais***

O principal elemento desenvolvido foi o Algoritmo de Shor, [2] um algoritmo quântico capaz de fatorar qualquer número em tempo exponencialmente menor do que um computador clássico, ameaçando, portanto, os métodos criptográficos assimétricos.

A dificuldade de fatoração desses números é evidenciada pela fórmula , que gera as chaves assimétricas, onde e são números primos com mais de 100 dígitos. Deste modo, o processo de fatoração de torna-se extremamente complexo [3].

Para verificação, desenvolveu-se um código na linguagem quântica Q#, processado por um Quantum Workspace dentro do simulador Azure Quantum, aplicando o algoritmo de Shor. Na linguagem Python (clássica), desenvolveu-se um código simples de fatoração, com o objetivo de comparar os tempos necessários para a fatoração em cada abordagem (clássica x quântica).

***3. Resultados***

Na tabela I, apresenta-se a fatoração de por meio do código clássico em Python, utilizando valores menores para tornar o estudo viável.

Tabela I – Tempo de fatoração de N utilizando a linguagem Python.

| Quantidade de algarismos de N | Tempo de execução do código |
| --- | --- |
| 8 | 0.441s |
| 9 | 1.505s |
| 10 | 29.165s |

É esperado que o tempo de execução aumente de acordo com a quantidade de algarismos. Ou seja, quanto maior o valor de , maior o tempo necessário para identificar os seus fatores e encontrar os valores de e , tornando inviável a fatoração de números com mais de 15 dígitos, por exemplo, em um computador clássico. Em contrapartida, na tabela II apresenta-se o mesmo processo, mas calculado por meio do algoritmo de Shor na linguagem quântica Q#.

Tabela II – Tempo de fatoração de N utilizando o algoritmo de Shor

| Quantidade de algarismos de N | Tempo de execução do código |
| --- | --- |
| 8 | 0.0289s |
| 9 | 0.0332s |
| 10 | 0.0397s |

Conforme a Tabela II, verifica-se que o algoritmo quântico é mais eficiente para encontrar os fatores de N, pois o tempo de execução do processo mostrou-se exponencialmente menor.

***4. Conclusões***

Considerando-se os resultados apresentados, conclui-se que a computação quântica possui uma eficiência notavelmente superior, e que possui um alto potencial para realizar a quebra de chaves criptográficas.

Apesar dos altos custos e das frequentes mudanças nas linguagens quânticas, a aplicação da computação quântica em escalas menores e com plataformas híbridas mostra-se viável. Com investimentos crescentes e avanços na pesquisa, é possível observar progressos notáveis em escalabilidade, estabilidade e disponibilidade de recursos quânticos, indicando um futuro promissor para aplicações disruptivas em diversos campos, beneficiando dessa maneira, a sociedade como um todo.

***5. Referências***

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

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

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