Hackathon Qiskit IBM

Grupo 3

Denise Sabgo	denise.sagbo@ufabc.edu.br	11980919843
Luiza Brittes Barros	luiza.brittes@aluno.ufabc.edu.br	11982351602
Victor Emanuel Guimarães	victoremanuelguima@gmail.com	11953991970
Nícolas Amaral Ferreira Pinho	nicolas.pinho@usp.br	21980389713

Projeto: Encontrar números gerados aleatoriamente utilizando o Algoritmo de Grover

Objetivo: Encontrar um número aleatório usando computação quântica

Em nosso projeto, implementamos o **Algoritmo de Grover** para realizar uma busca quântica em um espaço de soluções de tamanho 2^n, onde **n** representa o número de qubits. O objetivo é encontrar uma senha específica (ou estado alvo) com uma vantagem quadrática em relação à busca clássica.

O processo segue o seguinte fluxo de etapas:

1. Geração da senha

Geramos uma senha aleatória de ***n*** bits, que representa o estado que desejamos encontrar dentro do espaço de busca.

2. Inicialização do circuito

Criamos um circuito quântico com ***n*** qubits e aplicamos uma porta Hadamard (**H**) em cada um deles. Isso coloca todos os qubits em superposição uniforme, de modo que todas as possíveis combinações de bits (de 0 até $2\text{^}n$) possuem a mesma probabilidade inicial de serem medidas.

Matematicamente, o estado inicial após essa etapa é:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

3. Loop principal — Iterações de Grover

Nesta etapa, aplicamos repetidamente duas operações fundamentais do algoritmo:

a) Oráculo (Oracle)

O **oráculo** é uma operação quântica que marca o estado desejado invertendo o sinal da sua amplitude a partir da aplicação de uma fase.

$$|x\rangle \to \begin{cases} -|x\rangle, & \text{se } x = x_{\text{senha}} \\ |x\rangle, & \text{caso contr\#rio} \end{cases}$$

Na implementação, essa marcação é feita aplicando portas **X**, **H, X** e uma **porta multi-controlada (MCX)**, que atua apenas quando todos os qubits correspondem ao padrão da senha.

b) Diffusor (Diffuser ou Amplificador de Amplitude)

Após o oráculo, aplicamos o **difusor**, também conhecido como inversão sobre a média. Essa etapa amplifica a probabilidade do estado marcado e reduz a dos demais. Matematicamente:

$$D = 2|\psi_0\rangle\langle\psi_0| - I$$
$$|\psi\rangle \to D|\psi\rangle$$

Na prática, o difusor é implementado novamente com portas **Hadamard**, **X** e uma **central MCX**, espelhando a estrutura do oráculo, mas agindo sobre todos os estados.

4. Repetição

As etapas de **oráculo** e **difusor** são repetidas aproximadamente ***k*** vezes, onde ***k*** é dado por:

$$k_{\text{otimo}} \approx \frac{\pi}{4}\sqrt{2^n}$$

Esse número de iterações é o ponto ótimo que maximiza a probabilidade de medir o estado correto, conforme demonstrado matematicamente no algoritmo de Grover.

5. Medição e resultado

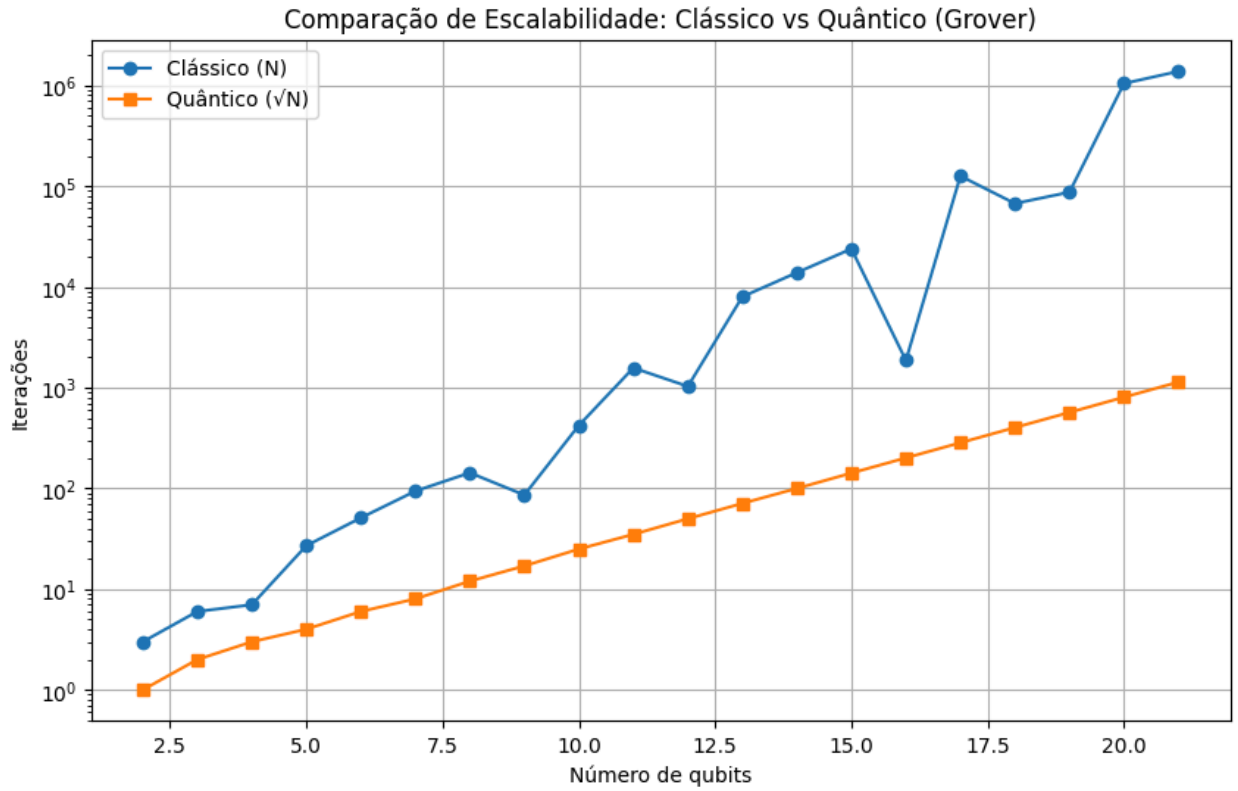
Por fim, medimos os ***n*** qubits. Com alta probabilidade, o resultado medido corresponde à senha original gerada no início do experimento. A probabilidade de acerto é dada por:

$$P(k) = \sin^2((2k+1)\theta)$$

Esse processo é comparado com uma busca clássica por força bruta, onde percorremos sequencialmente todas as possíveis senhas até encontrar a correta. O contraste entre ambos evidencia a vantagem quadrática da busca quântica.

Resultados e Discussão

Obtivemos, como esperado, uma **vantagem quadrática** aproximada em relação ao algoritmo clássico.



(Dados gerados pelo nosso simulador)

No entanto, a quantidade de qubits que podemos simular em um computador clássico é limitada pela grande quantidade de memória necessária. Mesmo assim, é possível observar como a Computação Quântica é extremamente eficaz e potencialmente mais eficiente do que a clássica.

Explorar as propriedades de onda dos qubits e utilizar sistemas quânticos para aproximar diferentes resultados pode nos ajudar a resolver cálculos extensos com diversas soluções em um tempo exponencialmente menor do que em computadores convencionais. Com isso, percebemos que a Física Quântica abre portas para áreas como Cibersegurança, Criptografia, Análise de Dados e Matemática Aplicada.

O tempo de simulação cresce exponencialmente com o número de qubits, e a simulação do algoritmo quântico tende a ser mais lenta em hardware clássico do que a busca clássica. Além disso, o ruído e as imperfeições físicas dos dispositivos quânticos reais podem reduzir a precisão das medições.

Trabalhos Futuros

Como extensão deste projeto, pretendemos implementar um sistema de senha quântica que aceite qualquer tipo de caractere, incluindo números, letras e símbolos especiais, ampliando o espaço de busca e aproximando o experimento de cenários reais de segurança digital.

Além disso, planejamos desenvolver um oráculo baseado em regras de validação, e não apenas na decodificação direta da senha, aproximando o modelo de problemas de verificação usados em sistemas criptográficos modernos.