No contexto das novas tecnologias e novos paradigmas computacionais que podem vir a substituir as atuais, a computação quântica destaca-se, dentre outros fatores, principalmente pela da melhoria na complexidade que alguns de seus algoritmos apresentam nas soluções de problemas comuns, a exemplo do problema de busca. Enquanto um computador quântico real ainda não é acessível, apesar de já existir, algoritmos quânticos podem ser criados tomando-se como base os princípios da mecânica quântica, um arcabouço matemático sobre o qual a computação quântica é definida.

Proposto por Lov Grover em 1996, o algoritmo quântico de busca utiliza o fenômeno da superposição da mecânica quântica, fato que o permite realizar uma busca paralela, sem replicação de hardware sobre uma base de dados desordenada. O critério de busca é representado em um sub-circuito denominado “oráculo”. Esse algoritmo tem complexidade O(sqrt(N)) se for executado em um computador quântico, no qual N é o número de elementos na base de dados. Isso representa um ganho polinomial sobre o melhor algoritmo clássico conhecido, o qual apresenta complexidade O(N) para o mesmo problema de busca.

Como prova de conceito, neste trabalho realizamos um estudo de caso para a raíz de uma equação do primeiro grau ($Ax + B = 0$). Tomando vantagem do fenômeno da superposição quântica, foi possível calcular o resultado da equação para todos os valores de X simultaneamente. Em seguida, como parte do algoritmo de Grover, iterativamente o estado do sistema quântico converge para a raiz da equação.

Neste estudo serão introduzidos os conceitos básicos da computação quântica: o qubit - sua unidade básica de representação de dados, os postulados da mecânica quântica - base teórica para a computação quântica, e o algoritmo quântico de busca proposto por Grover. Além disso, esse estudo trás uma breve descrição das portas quânticas utilizadas no estudo do caso desenvolvido.