

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

ERICK GALVÃO DA SILVA

LEONARDO RODRIGUES RIBEIRO

STHEFFANI GONÇALVES ROCHA EMBOAVA

ANÁLISE DE PLATAFORMAS E LINGUAGENS COMPUTACIONAIS PARA A MIGRAÇÃO DA TECNOLOGIA CLÁSSICA PARA A TECNOLOGIA QUÂNTICA

AMERICANA – SP

2023



CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

ERICK GALVÃO DA SILVA

LEONARDO RODRIGUES RIBEIRO

STHEFFANI GONÇALVES ROCHA EMBOAVA

Iniciação científica, sob a orientação da Prof. Dra. Mariana Godoy Vazquez

Área de concentração: Ciência da computação

AMERICANA – SP

2023

**RESUMO**

**ABSTRACT**

**SUMÁRIO**

[1. INTRODUÇÃO 3](#_Toc131845413)

[2. OBJETIVOS 3](#_Toc131845414)

[2.1. Objetivos Específicos 3](#_Toc131845415)

[3. JUSTIFICATIVA 3](#_Toc131845416)

[4. DESENVOLVIMENTO 3](#_Toc131845417)

[4.1. Implementação do Algoritmo de Deutsch-Josza 3](#_Toc131845418)

[4.2. Protocolos Quânticos e Algoritmo de Shor na Segurança da Informação 5](#_Toc131845419)

[4.3. Computação Quântica e Machine Learning 7](#_Toc131845420)

[5. CRONOGRAMA 8](#_Toc131845421)

[6. REFERÊNCIAS BIBLIOGRÁFICAS 10](#_Toc131845422)

# INTRODUÇÃO

# OBJETIVOS

## Objetivos Específicos

# JUSTIFICATIVA

# DESENVOLVIMENTO

## Implementação do Algoritmo de Deutsch-Josza

Com a constante evolução da Física e Computação Quântica é necessário compreender a lógica de programação deste novo paradigma, tendo ele três etapas: preparação dos estados iniciais, realização das transformações unitárias e execução das medições. Portanto abordaremos os conceitos de Computação Quântica e diferentes linguagens para implementações no simulador IBM Q Experience.

Para compreender a álgebra linear é necessário conhecer alguns conceitos matemáticos, como Espaço Vetorial Real, Subespaço Vetorial, Combinação Linear de Vetores, Produto Interno em Espaço Vetorial, Coordenadas Polares, Números complexos, Forma algébrica e Representação geométrica.

A Lei de Moore foi determinada pelo co-fundador da Intel Corporation, Gordon Earl Moore, formado em química e física, em um artigo escrito pelo mesmo e publicado pela revista Eletronic Magazine no ano de 1965. No artigo de sua autoria, ele conjectura sobre a evolução da tecnologia e a previsão para os anos futuros. Moore previu que a cada dezoito meses, a complexidade para a criação de processadores seria maior, a capacidade de processamento aumentaria em 100% e o custo permaneceria constante. Ou seja, o número de transitores em um processador dobraria, mantendo o mesmo custo e espaço. Os processadores passariam a ter capacidades maiores e melhores em um único “chip”. Essa previsão deu início a uma jornada de investimento em pesquisas e desenvolvimento, que possibilitou o alcance dessa meta. Porém, a Lei está entrando em obsolescência, pois em determinado momento será impossível aumentar a capacidade do processador e mantê-lo no mesmo espaço, tendo em vista que já estão sendo densenvolvidos processadores com transitores na ordem dos nanômetros.

Já Notação de Dirac ou Bra-ket é a mais usada para descrever sistemas mecânicos quânticos e também registradores quânticos. Espaço de Hilbert é um vetor espacial com um produto interno e uma regra definida pelo produto interno.

Em relação aos conceitos de computação quântica essenciais, temos a Sobreposição de estados que é a possibilidade dos *qubits* poderem existir continuamente em estados entre 0 e 1 e até serem estimulados. O Bit quântico (qubit) que pode ser encontrado nos estados 0, 1 ou em uma superposição entre os dois estados, sendo assim, pode existir nos dois estados ao mesmo tempo. No momento da medição do qubit, ele “se torna um bit clássico” pois não se pode ter os dois estados na medição, ele tem 50% de possibilidade de ser zero e 50% de possibilidade de ser um. É como uma foto de algo em movimento, mesmo que o objeto continue se movimentando, quando a foto é tirada, o objeto se mantém em apenas um lugar. Assim como o qubit quando é medido.

A Esfera de Bloch é a representação da tridimensionalidade de um qubit. Já as Portas quânticas são portas para manipulação de qubits, sendo as mais conhecidas Operadores de Pauli, Portas de Fase e Porta de Hadamard. O Algoritmo de Deutsch-Jozsa descreve um problema onde é necessário definir se uma função 𝑓(𝑥) é constante ou balanceada, e caso seja constante, todos resultados serão iguais a 0 ou iguais a 1.

Para finalizar temos os paradigmas de programação e os diferentes tipos de linguagem de programação, que servem para decompor o problema em uma série de funções, que recebem os inputs e produzem output, sem realizar mudança de estado internamente. Temos Haskell como a linguagem funcional mais conhecida e há linguagens multiparadigmas, em que é possível escrever programas que são procedurais, orientadas a objeto ou funcionais, como é o caso de Python, que possui uma sintaxe limpa e reputação de produtividade. Temos também a Quipper que é uma linguagem de programação funcional integrada para Computação Quântica sendo baseada em Haskell, portanto pode ser considerada como uma série de data types, combinadores e bibliotecas de funções Haskell.

## Protocolos Quânticos e Algoritmo de Shor na Segurança da Informação

A computação quântica é uma área de estudo multidisciplinar, a qual envolve as áreas de computação, física e matemática, e tem se tornado um elemento de estudo de grande destaque, por sua promessa de evolução, inovação e melhorias. As descobertas nas áreas “quânticas” permitem que as “clássicas” continuem se desenvolvendo, tendo em vista que um problema do passado pode ser resolvido através de um novo ponto de vista proporcionado pelos estudos em relação à computação quântica, que antes não se era conhecido.

Segundo NIELSEN & CHUANG, “os computadores quânticos vieram para resolver problemas que são impossíveis de serem resolvidos em computadores clássicos, não porque sejam insolúveis, mas sim pela grande quantidade de recursos necessários para a sua solução”.

A criptografia clássica, RSA, é baseada na função de Euler, que envolve a fatoração de grandes números primos. Essa fatoração, com a tecnologia clássica pode levar a centenas de anos para ser realizada, e a computação quântica promete solucionar esse problema rapidamente, através de algoritmos, por exemplo o algoritmo de Shor, onde as chaves de criptografia clássica podem ser decriptografadas em uma função de tempo muito menor através da descoberta do resultado da fatoração dos números primos.

Essa descoberta é um risco para segurança atual, pois ao considerarmos que todos os métodos de segurança são baseados na fatoração de grandes números primos por conta da sua complexidade de resolução na computação clássica, com a chegada da computação quântica essa “garantia” de segurança que tínhamos é perdida, e estamos todos sujeitos à diversos tipos de ataques, de modo muito mais rápido.

Para resolver essa deficiência na área de segurança, surge a criptografia quântica, que usa como princípios a Mecânica Quântica e o Princípio da Incerteza de Heisenberg.

A Criptografia Quântica se dá através da Distribuição de Chaves Quânticas (DCQ), que é um protocolo que permite que os bits da chave privada possam ser criados através de um canal público, entre dois parceiros. A segurança da chave que é gerada é garantida pelas propriedades da informação quântica e condicionada às leis da Física. O que impossibilita que a comunicação entre os dois parceiros seja interceptada sem que o espião seja descoberto, ou que o estado entre eles seja perturbado, e mesmo que o invasor consiga obter algum sucesso em alguma das etapas, as informações não podem ser clonadas, e isso é assegurado pelo Teorema de Não-Clonagem. O espião não consegue interceptar a comunicação sem ser percebido, e ao ser detectado (a taxa de ruído no canal seja maior que o limiar estabelecido), ambos os pontos irão alterar o protocolo no qual estão transmitindo.

Os protocolos quânticos de distribuição mais conhecidos são o BB84 e o B92. O BB84 foi o primeiro protocolo de distribuição a ser desenvolvido, sendo criado no ano de 1984, e se aproveita do fato de que é impossível medir uma informação quântica sem interferir em seu estado, impedindo que a comunicação seja interceptada por quem não faz parte da comunicação originalmente. O protocolo utiliza fótons polarizados para a transmissão das chaves, e esses podem ser medidos em três bases: vertical ou horizontal, circular (à esquerda ou à direita) e diagonal. O comunicador A irá escolher aleatoriamente em qual base irá modular o seu fóton: horizontal, vertical, circular à esquerda ou circular à direita, e o comunicador B, escolhe aleatoriamente qual polarização irá usar para medir o fóton que foi recebido, sem ter o conhecimento da base em que foi modulado. Se a base que B escolheu foi a mesma de A, os bits são lidos corretamente, se não, existe 50% de acerto de B. A e B fazem essa comunicação através de um canal público. B irá enviar a sequência que ele utilizou para A, que irá conferir quais medidas estão corretas. É a partir disso que é verificado se há interferência externa em uma comunicação, através de valores incoerentes (polarização correta e valor incorreto), caso não haja, a chave é segura. Se houver incoerências, os resultados são descartados e inicia-se uma nova tentativa de comunicação.

O protocolo B92, é baseado no protocolo BB84, porém utiliza outros estados e bases não ortogonais. Nele, serão utilizados apenas dois estados quânticos, ao invés de 4 como o protocolo anterior. Então, nesse protocolo haverá apenas duas possibilidades para os bits que são recebidos, e dado a sua simplicidade, os bits são considerados individualmente. B irá receber um valor em que o seu resultado poderá ser zero ou um, dependendo da base em que foi gerado. A e B geram duas sequências de bit aleatórios, e o que determina quando será zero e quando será um, depende da base que foi enviada: vertical ou horizontal. Por exemplo, se o resultado for zero, A envia vertical e quando for 1 envia diagonal. E B irá tentar detectar zero para diagonal e 1 para horizontal. Então, B irá verificar quais as posições que o bit foi detectado.

A Transformada de Fourier Quântica, nada mais é do que uma forma de resolver problemas complexos usando operações com resoluções conhecidas. Fourier descobriu que todo sinal poderia ser descrito como a soma de outros sinais que possuem frequência. Existem dois tipos, a Transformada Rápida, que é usada em computadores clássicos, e a Transformada de Fourier Quântica usada em computadores quânticos. A última (quântica), irá alterar as probabilidades de medir certo estado quântico. Ela serve de base para construção de outros algoritmos quânticos.

Em relação ao Algoritmo de Fatoração de Shor, ele é de grande importância para a computação quântica, pois resolve o problema de fatorar grandes números, problema estudado há muito tempo na matemática, tanto que esse método foi utilizado para o sistema de criptografia clássica, no sistema RSA. Sendo implementado na criptografia quântica, o algoritmo é capaz de resolver a fatoração de grandes números em segundos. E essa capacidade causa problemas aos sistemas de criptografia clássica, pois quebra chaves que foram construídas para levar anos para serem quebradas, em segundos. “O objetivo do algoritmo é achar o período de uma função, e na sequência, encontrar os fatores do valor solicitado.”

A criptografia clássica foi desenvolvida através de protocolos que visavam a dificuldade de fatoração de grandes números primos, o que inclusive era tema de estudo de matemáticos. A resolução ou a quebra das chaves geradas nesse princípio, na computação clássica, levaria centenas de anos para ser descoberta. Isso por conta da velocidade de processamento e da incapacidade da realização de vários testes ao mesmo tempo. Já a criptografia quântica possibilita a quebra dessa mesma chave em alguns segundos, o que se torna um grande problema na área de segurança de dados. Ou seja, a computação quântica surgiu através da necessidade de resolver problemas que são impossíveis de serem solucionados na computação clássica, e a criptografia quântica surgiu através da necessidade de segurança que são impossíveis de serem solucionados através da criptografia clássica.

## Computação Quântica e Machine Learning

O aumento na quantidade de dados está fazendo com que algoritmos de aprendizagem de máquina cheguem ao seu limite computacional, e é a partir desse limite que a computação quântica se mostra como uma possível solução para a ineficiência de processos realizados em um computador clássico.

Levemos isso em consideração: o melhor algoritmo de ML é, basicamente, aquele que melhor se ajusta aos dados e possui o menor tempo de execução (aprendizagem) e sabemos que dentro do Machine Learning, os dados de entrada são processados e organizados, para que como resultado seja gerado o que chamamos de previsão. O aumento do objeto processado (os dados) nos leva, portanto, ao problema de ineficiência dos algoritmos de ML Clássico devido ao tempo de execução muito alto.

Como solução, surge o Machine Learning Quântico. O QML possui a vantagem da aceleração quântica, que é definida pela complexidade de consulta, que dá nome à quantidade de vezes que o algoritmo consulta a fonte de informação, e pela complexidade de porta, que é a quantidade de operações elementares necessárias para executar o programa. Portanto, para saber se um algoritmo quântico é eficiente, é necessário tomar como base esses dois parâmetros, além de levar em conta os vários tipos de algoritmos de Machine Learning.

Contudo, a migração para o QML tende a ser longa devido aos problemas de entrada e saída de dados. Praticamente todos os dados atuais não estão em estado quântico, então para serem processados é preciso transformá-los. O uso da QRAM tem um custo muito alto e a transformação dos dados é extremamente demorada. Além dos problemas de entrada e saída, temos também o desafio da correção de erros quânticos, pois é preciso fazer ajustes nas portas para que a interferência seja minimizada e a eficiência otimizada.

Uma possível maneira de contornar o problema da transformação de dados, é reduzindo seu tamanho por meio da Análise de Componentes Principais, um método usado para reduzir a massa de dados sem que nenhuma informação seja perdida. A Análise transforma um conjunto de variáveis em outro conjunto de variáveis de mesma dimensão - são esses os componentes principais, e cada componente é uma combinação linear de todas as variáveis originais e mantém o máximo de informação possível.

Os algoritmos quânticos utilizados pelo ML são baseados nas técnicas de estimativa de fase, estimativa de amplitude e simulação hamiltoniana, e podem ser divididos em duas classes: a primeira classe de algoritmos é baseada na transformada quântica de Fourier de Shor e a segunda no algoritmo de Grover, que realiza a pesquisa quântica.

A Transformada de Fourier é essencial para o processamento de dados e é usada na maioria dos algoritmos contribui com a sub-rotina de estimativa de fase, que é usada na maior parte dos algoritmos quânticos pois permite encontrar autovalores de operações unitárias. O algoritmo de Grover é capaz de encontrar e ordenar um conjunto de dados cuja estrutura e organização são desconhecidos.

# CRONOGRAMA

|  |  |  |
| --- | --- | --- |
| DATA | ATIVIDADE | RESPONSÁVEL |
| Fevereiro/Março | O grupo se dedicou à revisão Bibliográfica dos 3 artigos (Implementação do algoritmo quântico Deutsch-Jozsa em linguagem funcional e no simulador IBM Q Experience, Aplicação de protocolos quânticos e algoritmo de Shor para a Segurança da Informação e Desempenho de algoritmos quânticos e clássicos em treinamento de Machine Learning supervisionado) e participou de reuniões e seminários semanais com a professora. | Erick Galvão, Leonardo Ribeiro e Stheffani Emboava |
| 29/03 | Apresentação da 1ª versão do cronograma de atividades | Erick Galvão, Leonardo Ribeiro e Stheffani Emboava |
| 04/04 | Pesquisas referente às plataformas, linguagens de programação escolhidas, repositórios e bibliotecas, e a implementação do algoritmo nas linguagens escolhidas (Java e Silq) | Leonardo Ribeiro  Erick Galvão |
| 05/04 | Apresentação da 2ª versão do Cronograma e reunião de alinhamento com a professora. | Erick Galvão, Leonardo Ribeiro e Stheffani Emboava |
| 07/04 | Início dos testes de implementação de circuitos quânticos nas plataformas Azure e IBMQ. Documentação dos testes realizados. | Leonardo Ribeiro |
| 07/04 | Pesquisas sobre o algoritmo de Shor. | Erick Galvão e Leonardo Ribeiro |
| 10/04 | Entrega e elaboração do primeiro relatório de atividades, contendo as revisões bibliográficas e o cronograma de atividades. | Stheffani Emboava  Erick Galvão |
| 24/04 | Entrega e elaboração do sexto relatório de atividades | Stheffani Emboava  Erick Galvão |
| 08/05 | Entrega e elaboração do sexto relatório de atividades | Stheffani Emboava  Erick Galvão |
| 22/05 | Entrega e elaboração do sexto relatório de atividades | Stheffani Emboava  Erick Galvão |
| 05/06 | Entrega e elaboração do sexto relatório de atividades | Stheffani Emboava  Erick Galvão |
| 19/06 | Entrega e elaboração do sexto relatório de atividades | Stheffani Emboava  Erick Galvão |

# REFERÊNCIAS BIBLIOGRÁFICAS

LACAVA, Lucas; MIANO, Mariana V. **Implementação do algoritmo quântico Deutsch-Jozsa em linguagem funcional e no simulador IBM Q Experience.** 2018. Revista Tecnológica da Fatec Americana, vol. 06 n. 2, abr/set de 2018. Disponível em: <https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/186>. Acesso em 14 fev 2023.

MIANO, Mariana V. **Aplicação de protocolos quânticos e algoritmo de Shor para a Segurança da Informação.** 2020. Revista Tecnológica da Fatec Americana, vol. 8 n. 01, 2020. Disponível em: <https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/233>. Acesso em 22 fev 2023.

MIANO, Mariana V. OLIVEIRA, Aleccheevina S. **Desempenho de algoritmos quânticos e clássicos em treinamento de Machine Learning supervisionado.** 2022. Revista Tecnológica da Fatec Americana, v. 9 n. 02 (2021). Disponível em: <https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/295>. Acesso em 6 mar 2023.