

# **COMPUTADORES CLÁSSICOS E QUÂNTICOS:**

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

**Gabriel R. Zsigmond**

INICIAÇÃO CIENTÍFICA



ESCOLA SUPERIOR DE PROPAGANDA E MARKETING

Sistemas de informação em comunicação e gestão

Brasil

05 de maio de 2020

**Gabriel R. Zsigmond**

# **COMPUTADORES CLÁSSICOS E QUÂNTICOS:**

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Projeto de Iniciação Científica para a Escola Superior de Propaganda e Marketing, sob a orientação do Professor Doutor Humberto Sandmann.

Orientador: Prof. Dr. Humberto Sandmann

Brasil

05 de maio de 2020

# **ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS:**

## **ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS**

**Gabriel R. Zsigmond**

### **Resumo**

O presente projeto, "Computadores Clássicos e Quânticos: Estudos, Implementação, Simuladores e Impactos Sociais", se propõe a estudar a história do computador e sua evolução. A mais recente inovação na área é a computação quântica, que certamente, inaugura a próxima geração de computadores. A computação quântica muda toda uma arquitetura na forma de computação, permitindo que os novos computadores sejam exponencialmente mais eficientes quando comparados aos mais modernos da atualidade. O projeto se propõe a entender e prototipar um computador tradicional de 8 bits em hardware, usando apenas portas lógicas simples, a fim de ilustrar, de forma clara, o funcionamento de um computador tradicional. Também, esse projeto busca entender e estimar as consequências sociais que os avanços da tecnologia e o desenvolvimento da computação quântica pode gerar. Entende-se que para essa análise, se faz necessário, inicialmente, uma ampla revisão bibliográfica, a fim de comparar esses dois tipos de computadores. Para ilustrar esta, será desenvolvida uma aplicação web que simula um computador tradicional e um computador quântico executando o mesmo algoritmo. É esperado que ao final do projeto, esse estudo traga um amplo e aprofundado conhecimento da área, além de, uma contribuição em relação ao impacto social do uso computação da quântica.

# Sumário

<b>1</b>	<b>Introdução</b>	<b>3</b>
1.1	Definição justificada dos objetivos e da sua relevância . . . . .	3
1.2	Metodologia a ser empregada . . . . .	5
<b>2</b>	<b>Computação Clássica</b>	<b>7</b>
2.1	A computação clássica e sua evolução . . . . .	7
<b>3</b>	<b>Computação Quântica</b>	<b>8</b>
3.1	A computação quântica e sua evolução . . . . .	8
<b>4</b>	<b>Computador</b>	<b>8</b>
4.1	Modulos . . . . .	8
4.1.1	Clock . . . . .	8
4.1.2	Materiais Necessários . . . . .	8
<b>5</b>	<b>Simulador</b>	<b>10</b>
<b>6</b>	<b>Criptografia</b>	<b>10</b>
6.1	Conceitos básicos de criptografia . . . . .	10
6.2	Criptografia aplicada computação clássica . . . . .	10
6.3	Criptografia aplicada computação quântica . . . . .	10
<b>7</b>	<b>Próximos passos</b>	<b>10</b>
7.1	Plano de Redação . . . . .	10
7.2	Cronograma . . . . .	10
7.3	Problemas . . . . .	10
<b>8</b>	<b>Reflexos sociais</b>	<b>10</b>
<b>9</b>	<b>Conclusões</b>	<b>10</b>
9.1	Perspectivas . . . . .	10

# 1 Introdução

## 1.1 Definição justificada dos objetivos e da sua relevância

A palavra computador é usada desde o século XVII, tendo a sua primeira referência escrita datada de 1613. No entanto, por muito tempo a palavra computador não tinha o mesmo significado que leva hoje. Até a década de 1940 a palavra “computador” era tida como uma profissão de alguém que calcula, segundo o dicionário Michaelis: “Aquele ou aquilo que calcula baseado em valores digitais; calculador, calculista”. [3]

Então o que é um computador no significado atual da palavra? Pode parecer uma pergunta simplista que não precisa ser respondida, porém, é uma pergunta para a qual muitas pessoas não sabem a verdadeira resposta. Computadores existem há muito mais tempo que o transistor <sup>1</sup> na forma mecânica e teórica. A definição real de um computador foi elaborada por Alan Turing (Reino Unido, 1912-1954), um matemático que se preocupava exatamente com a questão relacionada ao que era computável e o que não era. Ele descreveu uma máquina denominada Máquina de Turing. Seu trabalho foi submetido em 1936 e publicado no ano seguinte. Atualmente, desde o computador ou telefone celular em que você está lendo essa pesquisa até os supercomputadores, podem ser classificados como uma Máquina de Turing no nível mais simplista.

Uma máquina de Turing consiste em 4 partes: a fita, o cabeçote, a tabela e o registro de estado. Para visualizar a operação desta, primeiro é preciso imaginar uma tira de filme que se estende infinitamente em cada direção, agora imagine essa fita dividida em células e que cada célula possa conter apenas um de um conjunto definido de símbolos (como um alfabeto). Essas células podem ser reescritas por uma quantidade infinita de vezes, mas retêm suas informações indefinidamente até que sejam alteradas novamente. A parte da Máquina de Turing conhecida como cabeçote pode gravar símbolos nas células, além de aumentar ou diminuir sua posição na tira

---

<sup>1</sup>Um transistor é um dispositivo semicondutor usado para amplificar ou alternar sinais eletrônicos e eletricidade.

de filme por um número inteiro de células. A próxima parte é a tabela, essa contém um determinado conjunto de instruções para o cabeçote executar, como “mover para a esquerda 2 células” e “definir a célula para 7”. A última parte de uma máquina de Turing é seu registro de estado cujo objetivo é manter o estado atual da máquina. O estado inclui a instrução e os dados atuais na fita. [5]

O primeiro computador digital eletrônico de grande escala, foi criado em fevereiro de 1946 por cientistas norte-americanos, John Presper Eckert e John W. Mauchly, da Electronic Control Company . No final de sua operação em 1956, o ENIAC (Electrical Numerical Integrator and Calculator), continha 20.000 tubos de vácuo 7.200 diodos de cristal 1.500 relés 70.000 resistores 10.000 capacitores e aproximadamente 5.000.000 de juntas soldadas à mão. Ele pesava mais de 27 toneladas, tinha aproximadamente 2,4m \* 0,9m \* 30m de tamanho, ocupava 167 m<sup>2</sup> e consumia 150 kW de eletricidade. [5]

Apartir do ENIAC, as possibilidades tecnológicas tomaram uma nova proporção. Em 1969, apenas 13 anos após o desligamento do primeiro computador digital eletrônico, o computador de bordo da Apollo 11, missão que levou o homem a lua, tinha 32.768 bits [para uma explicação elaborada sobre bits refira-se ao capítulo 2 página 7] de RAM, o suficiente para armazenar um texto não formatado com cerca de 2.000 palavras. Em 2018, o iPhone XS, com 4GB de RAM (ou 34.359.738.368 bits), tem cerca de 1 milhão de vezes mais memória que o Apollo Guidance Computer. [4]

Durante o século XX, além do aumento de poder computacional dos dispositivos, outro fator impactante foi a redução de seus tamanhos. Assim, com tecnologias wearables <sup>2</sup>, os computadores se tornam ativamente presentes no cotidiano.

Levando em consideração o rápido avanço e desenvolvimento computacional, mencionados anteriormente, entende-se que os computadores agregam à sociedade, seja facilitando a comunicação e o compartilhamento de conhecimentos, como em outros aspectos. No entanto, a agilidade pela qual se deu tais transformações da tecnologia

---

<sup>2</sup>A tecnologia em questão não somente pode ser usada como uma peça de roupa ou um acessório, como também tem que possuir características que a conectem a outros aparelhos ou à internet.

da computação, também gera grandes expectativas e incertezas sobre o que ainda está por vir, tanto nas questões de mudanças tecnológicas quanto nos impactos relevantes na sociedade.

Tendo em vista a incerteza sobre o futuro da computação em relação aos próximos grandes avanços, nessa pesquisa serão estudados os conceitos da física clássica e da física quântica aplicados à computação, além disso, será estudado os princípios de criptografia <sup>3</sup>. Assim, a presente pesquisa irá prototipar um computador clássico de 8 bits em hardware usando apenas portas lógicas simples, dessa forma, ilustrando claramente o seu funcionamento. Junto a isso também será desenvolvida uma aplicação web que ilustre o funcionamento de um processador quântico. Ao final, conceitos de criptografia serão utilizados para exemplificar possíveis mudanças sociais que os próximos avanços tecnológicos podem gerar.

## **1.2 Metodologia a ser empregada**

Para a realização da pesquisa de iniciação científica, é indispensável o uso de pesquisa bibliográfica, assim recuperando conhecimento científico acumulado sobre o assunto. Segundo Telma Cristiane Sasso de Lima, o conhecimento da realidade não é apenas a simples transposição dessa realidade para o pensamento, pelo contrário, consiste na reflexão crítica que se dá a partir de um conhecimento acumulado e que irá gerar uma síntese, o concreto pensado [2]. E também a utilização do processo científico para a elaboração e efetivação do projeto em si. Ambas metodologias citadas acima, são cruciais para o desenvolvimento do relatório final na área de pesquisa em computação, já que na grande parte dos estudos científicos, a utilização do processo científico é frequentemente utilizada para um maior entendimento da obra e a construção do projeto se tornar mais facilmente executável.

Para o desenvolvimento da entrega do protótipo, computador de 8-bits, e para o simulador do computador quântico web, a principal metodologia utilizada será Project

---

<sup>3</sup>Criptografia é um sistema de algoritmos matemáticos que codificam dados para que só o destinatário possa ler.

Based Learnig (PBL). De acordo com David Van Andel, o PBL envolve os alunos em um processo rigoroso de investigação, onde eles fazem perguntas, encontram recursos e aplicam informações para resolver problemas do mundo real [1]. Assim, assumisse que esta é a melhor metodologia para desenvolver um protótipo físico de um computador e programar um site.



## 2 Computação Clássica

Computadores clássicos são todos aqueles que a maior parte da população mundial conhece, por exemplo computadores da Apple, Samsung, Dell dentre outros. É possível questionar o que todos esse tem em comum, a final todos possuem características bastante distintas. A resposta é bem simples, esses usam fenômenos da física clássica para operar. Assim, são classificados como computadores clássicos (ou binários), esses processam dois tipos de sinais, 1 e 0, ligado e desligado respectivamente. É com base nos bits <sup>4</sup> ligados e desligados que o computador baseia sua linguagem.

### 2.1 A computação clássica e sua evolução

---

<sup>4</sup>A menor unidade de informação que pode ser armazenada ou transmitida na comunicação de dados.

## **3 Computação Quântica**

### **3.1 A computação quântica e sua evolução**

## **4 Computador**

Construir um computador parece uma tarefa complicada e assustadora. Porém, uma CPU <sup>5</sup> é bastante simples em operação depois que os fundamentos por trás de todos os seus processos são compreendidos. Este capítulo destina-se a executar o passo a passo para que qualquer pessoa interessada seja capaz em construir seu próprio computador e obter o conhecimento que acompanha o processo.

### **4.1 Módulos**

Para facilitar o entendimento, e também o desenvolvimento do computador, este capítulo será dividido em alguns subcapítulos, assim cada um abordará uma parte do computador.

#### **4.1.1 Clock**

O clock do computador é uma parte essencial para o seu funcionamento. Este tem a função de sincronizar todas as operações. A ação mais rápida que o computador consegue executar é equivalente a uma vibração do seu clock.

#### **4.1.2 Materiais Necessários**

---

<sup>5</sup>CPU é a sigla para Central Process Unit, ou Unidade Central de Processamento. É o principal item de hardware do computador, que também é conhecido como processador, essa é a parte responsável por calcular e realizar tarefas determinadas pelo usuário.

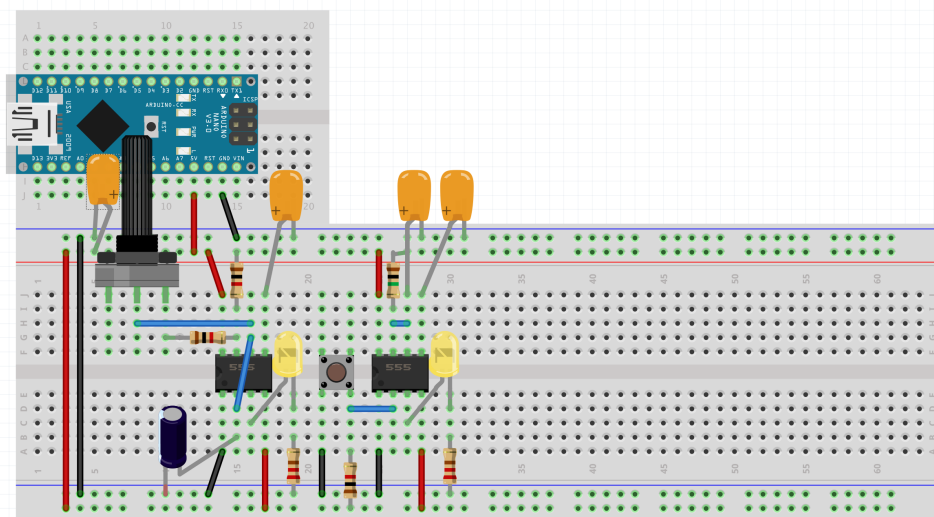


Figura 1: Esquema do Clock

## **5 Simulador**

## **6 Criptografia**

### **6.1 Conceitos básicos de criptografia**

### **6.2 Criptografia aplicada computação clássica**

### **6.3 Criptografia aplicada computação quântica**

## **7 Próximos passos**

### **7.1 Plano de Redação**

### **7.2 Cronograma**

### **7.3 Problemas**

## **8 Reflexos sociais**

## **9 Conclusões**

### **9.1 Perspectivas**

## Referências

- [1] Grand Rapids Business Journal – David Van Andel. Project-based learning is the future of education, out. 2019.
- [2] Telma Cristiane Sasso de Lima e Regina Célia Tamaso Mito. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. *Revista Katálisis*, 10(SPE):37–45, 2007.
- [3] Melhoramentos Ltda. – Michaels. Computador, out. 2019.
- [4] UOL – Bruno Santana. Iphone 6 é 120 milhões de vezes mais poderoso que o computador de bordo da apollo 11, jul. 2019.
- [5] Paul Wazlawick. *História da computação*. Elsevier, Rio de Janeiro, RJ, 2016.