ESCOLA CIDADÃ INTEGRAL TÉCNICA PREFEITO OSWALDO PESSOA
CURSO TÉCNICO EM MANUTENÇÃO E SUPORTE EM INFORMÁTICA
INTEGRADO A EDUCAÇÃO PROFISSIONAL

SYDNEY LOPES PAMPLONA

APLICAÇÃO DA COMPUTAÇÃO QUÂNTICA NA RESOLUÇÃO DE PROBLEMAS COMPUTACIONAIS E SEU IMPACTO NO ÂMBITO CIENTÍFICO

JOÃO PESSOA – PB
2018

SYDNEY LOPES PAMPLONA

APLICAÇÃO DA COMPUTAÇÃO QUÂNTICA NA RESOLUÇÃO DE PROBLEMAS COMPUTACIONAIS E SEU IMPACTO NO ÂMBITO CIENTÍFICO

Trabalho de Conclusão de Curso apresentado ao curso técnico em Manutenção e Suporte em Informática da Escola Estadual Cidadã Integral Técnica Prefeito Oswaldo Pessoa, como parte dos requisitos necessários à obtenção do diploma técnico.

Orientador: Prof. Esp. Carlos José Sabino Nascimento

JOÃO PESSOA

2018

SYDNEY LOPES PAMPLONA

APLICAÇÃO DA COMPUTAÇÃO QUÂNTICA NA RESOLUÇÃO DE PROBLEMAS COMPUTACIONAIS E SEU IMPACTO NO ÂMBITO CIENTÍFICO

Trabalho de Conclusão de Curso apresentado ao curso técnico em Manutenção e Suporte em Informática da Escola Estadual Cidadã Integral Técnica Prefeito Oswaldo Pessoa, como parte dos requisitos necessários à obtenção do diploma técnico.
Aprovada em: __/__/____.

BANCA EXAMINADORA

Prof. Esp. Carlos José Sabino Nascimento
Orientador

Prof. Creginaldo Silva
Examinador

Prof. Dhyego Santos
Examinador

Prof. Everton Gomes Mendes
Examinador

Dedico este trabalho a minha família, por terem me encaminhando e dado apoio nesta jornada a qual sinto prazer em terminar. Dedico também aos meus amigos que ficaram do meu lado até o fim dando incondicional apoio durante todo o tempo. Sem eles, faltar-me-ia sanidade para prosseguir no mundo acadêmico com o mesmo aproveitamento que tive. Muito sucesso em suas carreiras e também a esse tal de Pamplona. Muitíssimo obrigado a todos!

“Somente o desconhecido aterroriza os homens. Mas quando um homem encara o desconhecido, esse terror torna-se o conhecido.”

(Antoine de Saint-Exupéry)

RESUMO

A Computação Quântica é um campo de estudos em ascensão que contempla áreas de destaque, como a Matemática computacional, Física quântica e Ciência da Computação. Por estar imerso nas propriedades da mecânica quântica, o computador quântico apresenta um comportamento diferente do clássico. Suas diferenças são suas principais vantagens. A criação de um computador quântico perfeito pode liderar uma revolução no mundo em diversos aspectos, entender como ele funciona é crucial para entender o caminho que o mundo está tomando. Através de uma pesquisa qualitativa, é possível deduzir a carência de informação do público no que diz respeito a este campo de atuação. O trabalho também buscará introduzir aos leitores o tema e incentivar potenciais pesquisadores de um nível médio de ensino.

Palavras-chave: Computação Quântica. Mecânica Quântica. Revolucionar. Pesquisadores.

ABSTRACT

Quantum computing is a field of study on the rise that includes prominent areas such as computational mathematics, quantum physics and computer science. By immersing in the properties of quantum mechanics, the quantum computer behaves differently from the classical. Their differences are their main advantages. The quantum computer creation can leader the revolution in the world by several ways. Understand how it runs is crucial to understand the path the world is going. Through a qualitative research, it is possible to deduce a lack of information about the public with the study area. The work will also introduce the readers the theme and encourage potential researchers in high school level of knowledge.

Keywords: Quantum Computation. Quantum Mechanics. Revolutionize. Researchers

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

As primeiras propostas de um computador que utiliza os princípios da mecânica quântica começaram a surgir nos anos de 1980, desde então pesquisas no setor computacional quântico se intensificaram atraindo gradativamente a atenção do setor tecnológico e industrial. Os computadores quânticos diferem da computação convencional por aplicarem conceitos da Matemática, da Física e da computação em prática. (NICOLAU, 2010, p.1).

Segundo Mattielo, Silva, Amorim & Silva (2012), o campo de pesquisa da computação e informação quântica mostrou-se revolucionário ao levar em consideração que as conquistas e descobertas no domínio da mecânica quântica e da Ciência da Computação modificaram o estilo de vida do homem moderno em alguns aspectos. A computação clássica evoluiu o suficiente para demonstrar a humanidade o quão significativo foi a sua influência na sociedade moderna. É de se esperar que uma comercialização em grande escala de computadores quânticos revolucione ainda mais, em paralelo às descobertas que surgiriam com as novas pesquisas utilizando a tecnologia que lida com problemas em escala atômica.

O aprimoramento dos sistemas quânticos chegará a mudar os demais ramos de pesquisa, uma vez que, ela dá a possibilidade de resolver operações da mais alta complexidade como, por exemplo, interações moleculares e químicas, que resultariam consequentemente na descoberta de novas estruturas para auxiliar na criação dos novos materiais e medicamentos. Também possibilitaria cadeias de logística e de abastecimento ultra eficientes ajudando a encontrar novas maneiras de modelar os dados financeiros e isolar os principais fatores de risco, para fazer melhores investimentos. (MELLO, 2018).

Para mais aprofundamento na ciência, é necessário compreender um de seus alicerces que é a mecânica quântica, porém este trabalho analisará apenas os fundamentos que são advindos do pretexto científico computacional. Que é justamente um dos motivos para a Computação Quântica ser uma das ciências mais difíceis de se atuar, e também o motivo de ser bastante impactante no âmbito científico.

1.1. DELIMITAÇÃO DO TEMA E PROBLEMA DE PESQUISA

Este projeto de pesquisa delimitou-se em colher informações sobre como a aplicação da Computação Quântica na resolução de problemas computacionais pode influenciar o âmbito científico, seja com novas soluções para quaisquer tipos de problemas voltados nas diversas ramificações do ramo de pesquisas científicas, tendo como referência o Ensino Médio, etapa onde acontece o primeiro contato de estudantes com o mundo da Física de fato. Tendo como foco, estudantes situados no município de João Pessoa no ano de 2018.

1.2. JUSTIFICATIVA

A Computação Quântica é um ramo da ciência que está em ascensão e ainda carece de recursos do meio científico para o desenvolvimento de máquinas computacionais imersas nas propriedades da mecânica quântica. A computação clássica foi desenvolvida sob as condições da Física clássica, diferentemente da Computação Quântica, que abrange muito mais a Física moderna. No momento em que tais propriedades estiverem bem aplicadas o computador quântico se tornará um importante agente na evolução tecnológica humana. A eficácia em trabalhar com a informação abrirá portas para que outras tecnologias se tornem mais perfeiçoadas através de questões problemáticas, que o processamento de um computador comum não seria capaz de computar, solvidas por um aparato quântico.

Os computadores com características quânticas poderão assim, aposentar os tradicionais, por razão da maneira como eles funcionam. Em questão à segurança, a criptografia de sistemas públicos teria de ser revista graças ao poder do Q-bit. Um computador com 49 Q-bits perfeitos é o bastante para superar um computador binário tradicional, suscitando a supremacia quântica. (GRIMES, 2018).

Com a contribuição de diversos físicos e pesquisadores renomados no meio acadêmico, a Física fora capaz de progredir. É notório a necessidade que o campo da Computação Quântica possui de estudos focados para colaboração com novas aplicações da teoria quântica.

1.3. OBJETIVOS

1.3.1. Geral

Identificar a influência da Computação Quântica explorando suas aplicações práticas – tal como na resolução de operações matemáticas de caráter científico –, expor o potencial que o setor dispõe através de seus principais fundamentos, que é o princípio da mecânica quântica e enfatizar o impacto desta ciência para a sociedade.

1.3.2. Específicos

- Explicar os fundamentos da mecânica quântica;
- Expor as principais propriedades para a resolução de problemas com o aparato quântico computacional;
- Comparar aplicações da Computação Quântica para destacar seu impacto no mundo científico;
- Mostrar a carência de informação do público jovem de estudantes.

1.4. CRONOGRAMA

Cronograma – ano 2018

Atividades	Agosto	Setembro	Outubro	Novembro	Dezembro
Pesquisa bibliográfica e documental	**x**	**x**	**x**	**x**	**x**
Discussão teórica em função dos objetivos	**x**	**x**	**x**	**x**	
Determinação de categorias para realização da pesquisa de campo	**x**	**x**			
Execução da Pesquisa de campo	**x**	**x**	**x**	**x**	**x**
Análise dos resultados	**x**	**x**	**x**	**x**	**x**
Redação da Monografia		**x**	**x**	**x**	**x**
Revisão Final da Monografia					**x**
Banca Pública					**x**

1.5. PROCEDIMENTOS METODOLÓGICOS

O trabalho reconhece o cerne da Computação Quântica e os demais setores em alcance do mesmo. Para este tipo de pesquisa, será utilizado o método qualitativo (GERHARDT & SILVEIRA, 2009), o qual não se limita a representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc.

O trabalho contará com uma pesquisa exploratória tendo como base, fontes bibliográficas primárias e secundárias. Segundo Marconi & Lakatos (2003):

> A pesquisa bibliográfica, ou de fontes secundárias, abrange toda bibliografia já tomada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico etc. (MARCONI & LAKATOS, 2003, p.183).

Serão coletados os principais rudimentos que ligam a Física moderna, a Ciência da Computação e os elementos da Computação Quântica, tendo um aprofundamento nos conceitos e leis aplicadas a mecânica quântica, mas não se submetendo a comprovação dos mesmos.

Por fim denotar a importância da expansão deste campo de estudos e expor a desinformação dos novos estudantes em relação ao tema por meio de um questionário específico.

Formando as seguintes etapas:

- Exibir o embasamento que a área da Computação Quântica denota que é a mecânica quântica;
- Mostrar as principais características da Computação Quântica;
- Expor as principais aplicações do computador quântico e sua importância no âmbito científico.

1.6. ORGANIZAÇÃO DO TRABALHO

Para atender os itens destacados anteriormente, o trabalho será gerenciado conforme o indicado:

No Capítulo 2 são apresentados os principais conceitos da Ciência da Computação que estão destinados a aparecerem no decorrer do trabalho.

No Capítulo 3 começa o embasamento teórico no que denota os efeitos e ocorrências da mecânica quântica presentes na Computação Quântica. Um capítulo inteiramente voltado para os aspectos da Física moderna.

O Capítulo 4 é voltado para a Computação Quântica, demonstrando sua eficiência na resolução de problemas ao expor os principais algoritmos.

O Capítulo 5 contempla as principais aplicações dos computadores quânticos e o impacto que estes causam no âmbito. Também enfatiza a necessidade de ser uma área mais abrangente no Ensino Médio.

O Capítulo 6 apresenta as considerações finais e perspectivas para o futuro no que diz respeito ao tema.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. CIÊNCIA DA COMPUTAÇÃO

A humanidade sempre buscou uma maneira de otimizar suas tarefas por meio da tecnologia, a exemplo da criação de máquinas para automatização dos cálculos matemáticos responsáveis por estabelecer a Ciência da Computação. O primeiro grande marco computacional aconteceu durante o período da Segunda Guerra Mundial, quando o matemático e criptoanalista britânico Alan Turing desenvolveu uma das primeiras máquinas computacionais a fim de descriptografar mensagens inimigas interceptadas pelo governo americano. O campo de estudos da Ciência da Computação tornou-se finalmente independente na década de 1960, desde então explorando novos horizontes. (FILHO, 2007, p.23, 74-78). Atualmente, a Ciência da Computação abrange ramos da: Matemática computacional, Engenharia de *hardware* e *software* e até mesmo Ciências Naturais. (KON, 2016).

2.1.1. Software

O computador é formado por dois principais elementos conhecidos como *software* e *hardware*. Ambos construídos por engenheiros e programadores da área a fim de apresentar uma solução de uma problemática. Na Ciência da Computação, o *software* é conhecido por representar a parte que lida com soluções lógicas no computador, ou seja, os programas. Um programa é uma sequência de algoritmos definidos pelo programador para chegar num objetivo específico. O termo em inglês "*Soft*" faz alusão a facilidade com que esta parte do computador tem para ser modificada. (BRITO, p.19). Resolver um problema de *software* é bem mais possível do que resolver um problema de *hardware* em um computador. Pois o programador trabalha inteiramente com as linhas de programação, averiguando e corrigindo instruções errôneas pós identificação.

2.1.2. Hardware

O *hardware* do computador também pode ser descrito como a parte física da máquina. Exatamente por ser a parte física que o termo "*Hard*" foi utilizado, pois assemelha-o com a parte mais rígida a ser modificada no computador. Uma vez danificada, para resolver um problema no *hardware* é ainda mais complicado que no *software*. (BRITO, p.19).

2.1.3. Unidade Central de Processamento

Todo computador funciona a base de uma Unidade Central de Processamento (UCP), *hardware* considerado como o "cérebro" da máquina. Os chamados microprocessadores são chips que concentram os principais componentes do computador: a **Unidade de Controle** (UC), responsável por controlar o fluxo de dados nos barramentos do computador e da ULA, a **Unidade de Lógica e Aritmética** (ULA), responsável por processar operações lógicas e aritméticas dos dados que passam por ela, e os **Registradores**, que são memórias ultrarrápidas auxiliares da ULA, servindo para armazenar dados a serem trabalhados pelo processador. (FÁVERO, 2011, p.47, 57). Por meio das operações lógicas os processadores calculam os 0's e 1's, originados da linguagem de programação *Assembly*[1]. (BRITO, p.13).

2.1.4. Transistor

Os transistores são componentes eletrônicos de escala nanométricas responsáveis por representar dados e fazerem as operações lógicas e aritméticas do computador. Devido ao tamanho que o transistor vem abarcando com o aprimoramento da nanotecnologia, um único processador é capaz de envolver bilhões de transistores em seus chips, onde cada transistor representa um bit (menor parte da informação) que pode assumir os valores "0" para ausência de energia e "1" para presença de energia, assim, um processador é capaz de realizar estes ciclos bilhões de vezes por segundo, ou seja, na frequência de GHz (Giga Hertz). Os transistores reaproveitam as cargas de energia passando de um para outro, tornando-os capazes de realizar operações lógicas básicas. (BRITO, p.6-8).

[1] O sistema de numeração binário do Assembly foi adotado pela facilidade na representação elétrica.

2.1.5. Circuitos Lógicos

Os transistores presentes nos circuitos eletrônicos do microprocessador realizam operações lógicas e aritméticas a partir dos sinais binários que eles carregam. Na estrutura de um transistor encontramos estruturas conhecidas como portas (*gates*) lógicas, responsáveis por permitir ou não a passagem de energia. Os circuitos que carregam estas portas são conhecidos como circuitos lógicos. As portas lógicas são a base para a construção dos algoritmos de qualquer sistema digital, pois desempenham operações aritméticas como soma, multiplicação e algumas comparações. (MONTEIRO apud FÁVERO, 2011, p.35-36).

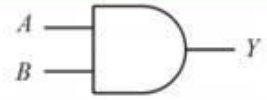
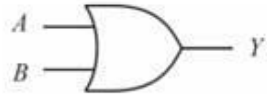
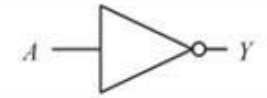
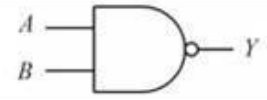
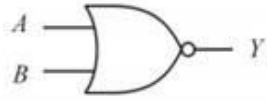
Operadores	Simbolo	Equação Booleana
E "AND"		$Y = A \cdot B$
OU "OR"		$Y = A + B$
NÃO "NOT"		$Y = \overline{A}$
NÃO E "NAND"		$Y = \overline{A \cdot B}$
NÃO OU "NOR"		$Y = \overline{A + B}$

Figura 1 *– Portas lógicas mais usadas (AND, OR, NOT, NAND e NOR)*
Fonte: (analiseedesenvolvimento.wordpress.com)

2.2. MECÂNICA QUÂNTICA

A mecânica quântica é uma das teorias físicas mais bem-sucedidas. Ela faz parte da Física moderna, originada dos estudos da Física quântica, onde tem seus estudos voltados para o mundo atômico e molecular. (OLIVEIRA & SARTHOUR, 2004, p.2). Ao contrário de outras teorias esta prevalece em constante aprimoramento devido o mundo de incertezas que apresenta.

3. A TEORIA QUÂNTICA

3.1. DO TRANSISTOR AO ÁTOMO

A invenção do transistor [2.1.4] como semicondutor de eletricidade foi o marco mais importante na evolução da eletrônica. A partir dele, o que antes eram computadores enormes graças ao sistema rústico de medição binária por meio de válvulas, reduziu consideravelmente de tamanho quando os circuitos integrados[1] passaram a preponderar nas novas unidades de processamento, chamados de microprocessador. De acordo com Mehl:

> Na década de 1960 as válvulas a vácuo vinham sendo rapidamente substituídas pelos transistores. Além do custo de fabricação cada vez mais baixo, os transistores mostravam-se com tempo de vida mais longo que as válvulas e permitiam a fabricação de equipamentos menores e mais confiáveis. (MEHL, p.10).

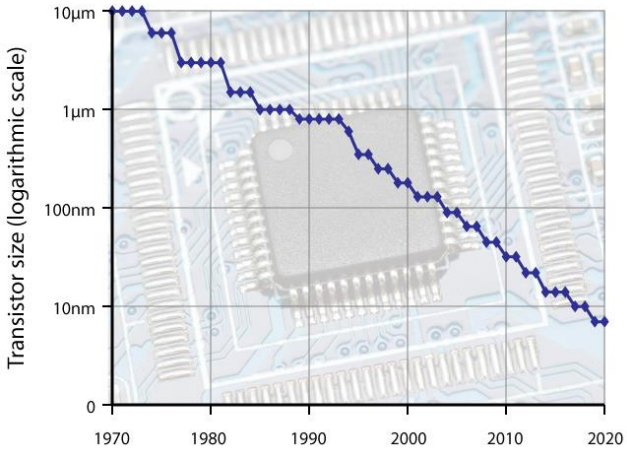


Figura 2 *– Tamanho dos transistores (escala logarítmica)*
Fonte: (futuretimeline.net)

Com componentes cada vez menores a computação convencional mostrou-se em constante aprimoramento. A era dos transistores começou e graças a evolução da eletrônica os computadores puderam aproximar-se do auge de sua magnificência. Na década de 1960, Gordon Moore, fundador da empresa norte-americana de microprocessadores Intel, observou que o tamanho dos transistores de um microprocessador diminuiria a metade a cada 1 ano e meio. Advindo dessa otimização

[1] Conjunto de transístores, diodos, resistências e condensadores fabricados num mesmo processo. Também conhecido como chip.

no tamanho dos transistores, temos microprocessadores possivelmente menores e com mais circuitos integrados disponíveis para operações mais complexas. (MEHL, p.11). A lei de Moore também revelou que dentre alguns anos o transistor, ou o dispositivo que ficara encarregado de representar o bit, diminuiria até que chegasse ao tamanho de um único átomo. Visto que o seu decrescimento exponencial representaria a necessidade de menos átomos na materialização do mesmo dispositivo. Neste ponto, as leis da Física quântica atuariam sobre ele.

> Do ponto de vista físico, a Lei de Moore impõe um limite natural aos computadores, pois a partir do momento que fosse atingido o limite de um bit por átomo, não haveria mais como aumentar a densidade de bits por chip. Contudo, quando a escala atômica for atingida, o paradigma clássico da máquina de Turing deixa de ser válido, ou seja, devemos pensar num modelo de computação baseado nas leis da mecânica quântica. É justamente neste ponto que surge o que chamamos de Computação Quântica. (MATTIELO, SILVA, AMORIM & SILVA, 2012, p.34).

3.2. LEI DE PLANCK

De acordo com Brennan (2003), com base em estudos dos efeitos fotoelétricos que aconteciam ao submeter um corpo negro[1] a luz, o físico e teórico alemão Max Planck propôs-se a introduzir uma ideia completamente nova para justificar a irradiação mutável que o corpo negro emanava ao ser exposto por altas ou baixas temperaturas. Planck sugeriu que a radiação existia em pequenas unidades ou pacotes, essa unidade de energia viera a ser chamado de *quantum* (palavra latina para "quanto"). E o que definiria a quantidade de energia destes *quanta* seria o comprimento de onda da radiação. A partir desta relação, criou-se a seguinte equação:

$$E = \hbar f \quad (1)$$

Um *quantum*, $\boldsymbol{E}$, é igual à frequência da radiação, $\boldsymbol{f}$, vezes a constante de Planck, $\boldsymbol{\hbar}$.

A teoria dos *quanta* de Planck marcou o início da Física moderna. Conforme surgiam novos estudos sobre a luz e o mundo atômico, as implicações da Lei de

[1] Corpo negro é um objeto hipotético que absorve toda a radiação eletromagnética que nele incide: nenhuma luz o atravessa e nem é refletida.

Planck surtiram um efeito mais do que o esperado, se tornando futuramente a raiz da teoria quântica. (BAKER, 2015, p.17).

3.3. DUALIDADE ONDA-PARTÍCULA

O físico alemão Albert Einstein é bastante apontado na contribuição aos estudos da luz por ter relacionado este tipo de radiação com os quanta de Planck, criando os fótons, porém Einstein também contribuiu com estudos a outros tipos de radiação, como os raios-X e raios γ (gama). No início do século XX, muitos físicos centraram suas pesquisas nos raios-X, onde começaram a surgir conceitos dualísticos a respeito da radiação e sua natureza quântica, se eram ondas de alta frequência ou pulsos não-periódicos curtos. Com a descoberta da difração[1] de raios-X por cristais, ficou claro que os raios-X possuíam propriedades ondulatórias, porém isto aumentou o debate de questões de interpretação corpuscular ou ondulatória dos raios-X. (ROSA, 2004, p.13-33).

Combinando a fórmula de Einstein, que relacionava massa e energia, e a fórmula de Planck, que relacionava frequência e energia, o físico francês Louis De Broglie mostrou em sua tese de doutoramento que a onda, assim como a partícula, apresentava a condição de dualidade onda-partícula, onde ambas assumiam propriedades ondulatórias e corpusculares simultaneamente. Associando uma onda para toda e qualquer partícula. (BRENNAN, 2003, p.177-181).

> Minhas pesquisas sobre a física dos raios-X me haviam convencido da necessidade de uma teoria sintética das radiações combinando o aspecto "onda" e o aspecto "fóton", e eu havia refletido muito sobre os trabalhos já antigos do Sr. Einstein sobre os quanta de luz. Meditando sobre essas questões, fui levado a fazer em 1922 duas publicações sobre esse assunto. (DE BROGLIE apud ROSA, 2004, p.86).

Experimentos feitos pelos cientistas Clinton Davisson e Lester Germer comprovaram a tese de De Broglie a partir da observação do caráter ondulatório do elétron, uma partícula subatômica, incidindo-o em um feixe de energia definida num cristal de níquel. Os átomos do cristal de níquel atuam como centros de difração,

[1] A difração é um fenômeno físico que ocorre em qualquer tipo de onda. Acontece quando a onda gera um desvio de sua trajetória retilínea após ela passar pela aresta de um objeto.

espalhando o feixe de elétrons incidentes em direções muito características, assim como na difração de raios-X por um sólido. (AEGERTER, SIU LI, MUNTE & ZANATTA, 2013, p.1).

$$\lambda = \frac{\hbar}{mv} \tag{2}$$

O comprimento de onda de De Broglie, λ, é igual a constante de Planck, $\hbar$, sobre a massa, m, vezes a velocidade, v.

3.4. PRINCÍPIO DA INCERTEZA

O Princípio da Incerteza de Werner Heisenberg traz consigo uma nova filosofia para os físicos, pois as características que marcavam o determinismo da Física clássica de Newton foram abandonadas para se ter uma nova compreensão de como a interpretação probabilística é um elemento fundamental na mecânica quântica. A mecânica clássica dispõe de equações que determinam na mais inteira certeza a posição e o momento de um corpo para todos os valores do tempo, estas que foram provadas com grande exatidão, até os estudos com partículas atômicas mostrarem que tais equações são adequas apenas no mundo macroscópico. (EISBERG & RESNICK, 1979, p.97-99).

No mundo microscópico o Princípio da Incerteza revela que é impossível discernir com clareza a posição e o momento de um objeto quântico, relacionando-os como grandezas inversamente proporcionais sabemos que o quão maior for a precisão de um, menor será a precisão do outro. Por esta correlação matemática, faz-se necessário utilizar de funções probabilísticas, para determinar as chances da posição ou do momento (massa de um corpo em relação a sua velocidade) que o objeto quântico vai se encontrar. (NOVAES & STUDART, 2016, p.33-34).

A compreensão desta incerteza se deu graças a tentativas teóricas para medir o movimento de uma partícula subatômica, como um nêutron. Heisenberg viu que para observar o comportamento desta partícula, seja qual fosse o instrumento utilizado, ele interferiria em sua trajetória. Alega Baker (2015, p.70):

> Um radar poderia rastrear a partícula, ao refletir ondas eletromagnéticas nela. Para uma precisão máxima, seria preciso usar raios gama, que têm comprimentos de onda muito curtos. Entretanto, por causa da dualidade onda-partícula, o raio gama que incide sobre o nêutron atuaria como uma rajada de

> fótons-bala [...] quando um fóton poderoso atingisse o nêutron, ele lhe daria um grande impulso que alteraria sua velocidade. (BAKER, 2015, p.70).

Seguindo este exemplo, se usássemos fótons com ondas maiores e de menos energia, nota-se que ele deixaria de influenciar na velocidade do nêutron para acarretar numa mudança da posição do átomo, ofuscando a precisão de suas coordenadas. (BAKER, 2015, p.69-70). Portanto o princípio da incerteza demonstra a impossibilidade na obtenção de resultados precisos ou melhores além dos que a sua equação pode oferecer, como resultado da inevitável interação entre o observador e o observado. (EISBERG & RESNICK, 1979, p.100).

$$\Delta x \cdot \Delta Q \geq \frac{\hbar}{4\pi} \tag{3}$$

A incerteza da posição, Δx, vezes a incerteza do momento, ΔQ, é maior ou igual a constante de Planck, $\hbar$, sobre **4** vezes Pi, π.

3.5. SUPERPOSIÇÃO DE ESTADOS

Na computação clássica nos deparamos com um mecanismo operante na base binária que oferece apenas uma possibilidade como resultado de sua ação. Tal como o ato de jogar cara ou coroa, onde uma moeda só pode apresentar uma de suas duas faces. Porém na mecânica quântica não trabalhamos com valores exatos, sempre há imprevisibilidade ao determinar o estado de uma partícula. Supondo que joguemos cara ou coroa com uma moeda nas propriedades da mecânica quântica, o resultado obtido seria o equivalente a cara e coroa simultaneamente, esta medição é chamada de superposição ou sobreposição. (MATTIELO, SILVA, AMORIM & SILVA, 2012, p.5).

> O princípio da superposição diz que o estado de um sistema físico pode ser escrito como uma combinação linear de outros estados e essa propriedade só existe no reino da mecânica quântica. (BAKER, 2015, p.70).

Para melhor compreensão, o físico austríaco Erwin Schrödinger desenvolveu um experimento mental aplicando a superposição de estados quânticos no mundo macroscópico, conhecido como o paradoxo do Gato de Schrödinger. Neste experimento um gato é posto dentro de uma câmara de aço, onde há um contador

Geiger[1] que carrega uma pequena quantidade de material radioativo, tão pequeno que a probabilidade de um de seus átomos se decompor no curso de uma hora é de 50%. Se a desintegração do material radioativo ocorrer, o contador aciona um relé que ativa um martelo, quebrando um frasco de ácido cianídrico e matando o gato dentro do compartimento. (DUPRÉ, 2009, p.49). Após uma hora não teremos certeza se o gato estará vivo ou morto, pois as chances são iguais para ambos os estados. A situação em que o gato se encontra pode ser descrita como a superposição de estados, afinal o animal se encontrará num estado de vivo e morto simultaneamente até que um observador interaja com o compartimento, difundindo seu estado entre vivo ou morto. (GRECA & HERSCOVITZ, 2005, p.4).

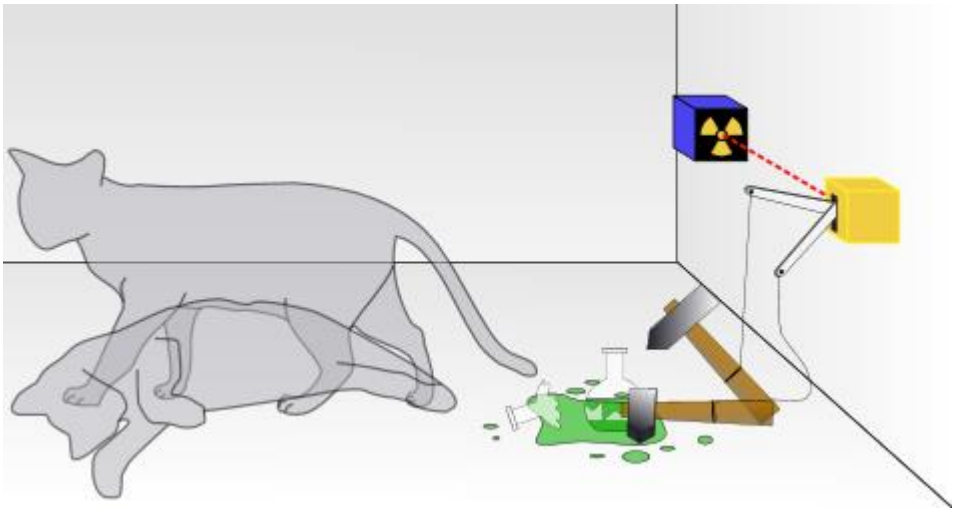


Figura 3 *– Diagrama do experimento mental do gato de Schrödinger*
Fonte: (wikipedia.org)

3.6. EMARANHAMENTO DE ESTADOS QUÂNTICOS

Indispensável para a Computação Quântica, o emaranhamento (ou correlação) é um efeito quântico enigmático para a maioria dos cientistas do século XX que se propuseram a desenvolver a teoria. Tão peculiar que o próprio Einstein a denominou como “ação fantasmagórica a distância”. (FREIRE, PESSOA & BROMBERG, 2011, p.68). Sua ação consiste em correlacionar o estado (medidas possíveis) de uma partícula a outra, independentemente da distância ou lugar que se encontram.

[1] O Contador Geiger serve para medir certas radiações ionizantes (partículas alfa, beta ou radiação gama e raios-X).

Num sistema com duas ou mais partículas emaranhadas torna-se possível prever pelo menos o estado de uma delas, por exemplo: Correlacionando um par de elétrons **A** e **B**, levando em consideração apenas os *spins*[1] de seu estado, ao observar que o elétron **A** está com o *spin* para cima, instantaneamente o elétron **B** ficará com o *spin* para baixo. (NOVAES & STUDART, 2016, p.116).

3.6.1. Teleporte Quântico

O emaranhamento também é utilizado para transferir propriedades de uma partícula para outra. Neste caso, uma das vantagens do emaranhamento, que é a ação instantânea da mudança de estados, não é devidamente aproveitada em trocas de informações. Para transferir as propriedades de uma partícula, deve-se levar em conta a superposição da partícula. (NOVAES & STUDART, 2016, p.123).

A partícula é capaz de assumir mais de um estado simultaneamente, e o ato de medir uma partícula emaranhada influenciará diretamente na outra. Ou seja, para a troca de informações ser concluída com sucesso, a pessoa que vai emitir a informação por meio do teleporte deverá comunicar ao receptor o seu estado para que o receptor saiba se as propriedades apresentadas em sua partícula constam com as da partícula emissora. (OLIVEIRA & SARTHOUR, 2004, p.14).

A troca de informações ocorre sobre mesma condição dos meios comuns de comunicação, isto tira a principal vantagem do emaranhamento, que é a rapidez na mudança de estados.

3.7. DESCOERÊNCIA QUÂNTICA

Outro efeito da mecânica quântica atrelada a Computação Quântica é o fenômeno de descoerência. O efeito de descoerência pode ser entendido como uma consequência das propriedades eminentes da partícula no mundo quântico. Como anteriormente dito, a mecânica quântica não trabalha com valores propriamente exatos, diferentemente da mecânica clássica, que oferece predições satisfatórias em sistemas aplicados ao mundo macroscópico. Isto ocorre, pois, à medida que um

[1] O elétron produz um campo magnético ao girar, este movimento de rotação é chamado de spin. Ele pode girar para os dois sentidos, horário e anti-horário.

sistema aberto é isolado do meio ambiente e é tratado singularmente como uma partícula, a medição o faz perder a exatidão de propriedades como posição e trajetória. (FREIRE, PESSOA & BROMBERG, 2011, p.69).

O efeito de descoerência é justamente a transição entre o indeterminismo para o determinismo nos sistemas quânticos. A dualidade onda-partícula mostra que não é possível que um objeto quântico – seja ele composto por fótons ou átomos – em superposição sofra medições exatas de seu comportamento. Como evidenciado no experimento do Gato de Schrödinger, a medição do sistema colapsa a superposição e mostra um dos possíveis estados. (NOVAES & STUDART, 2016, p.122). O efeito da descoerência é uma das principais dificuldades dos físicos na utilização efetiva do emaranhamento, pois a dificuldade em isolar e medir perfeitamente um objeto quântico ainda reina no século XXI.

4. COMPUTAÇÃO QUÂNTICA

Em 1980 surgiram dois importantes campos de pesquisa voltados para o domínio da mecânica quântica: a informação quântica e a Computação Quântica. Ambos com o intuito de aplicar os sistemas quânticos num aparato computacional, para a manipulação de informações. (GRECA & JUNIOR, 2013, p.15).

4.1. BIT QUÂNTICO

Segundo Oliveira & Sarthour (2004), o computador clássico utiliza a unidade de informação *bit* a partir de um sistema binário onde os componentes eletrônicos da unidade de processamento assumem valores lógicos de: “0” para a ausência de corrente elétrica e “1” para a presença de corrente elétrica. Contudo, quando se trata de Computação Quântica, a unidade de informação com características quânticas é o Q-bit (Bit Quântico). O Q-Bit pode apropriar-se do efeito de superposição com os dois valores lógicos, fazendo-o assumir posições como “0” ou “1”, e também “0 e 1” simultaneamente, gerando um ganho exponencial de variantes a cada Q-bit adicionado ao sistema.

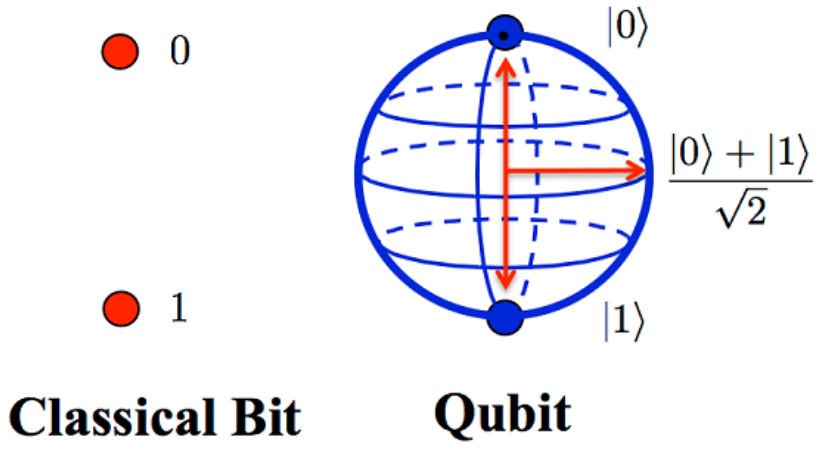


Figura 4 *– Representação dos estados do Bit clássico e do Bit quântico*
Fonte: (eyerys.com)

Os Q-bits são formados por diferentes tipos de objetos quânticos, de modo que passem a representar um valor. Dependendo do objeto, eles terão vantagens e desvantagens. Alguns, como os fótons, são melhores para comunicação; outros, como a matéria, são melhores para o processamento. Outro fator importante é que alguns oferecem mais resistência a descoerência quântica e outros são mais

sensíveis ao ambiente. (RUSSON, 2017). De acordo com Oliveira & Sarthour (2004), os objetos mais utilizados são:

- Estados de polarização dos fótons;
- Estados eletrônicos em átomos;
- Elétrons em poços quânticos;
- Estados de pares de Cooper em supercondutores.

Em sistemas com poucos Q-bits utilizam-se de técnicas como ressonância magnética nuclear e armadilha de íons para fazer as medições. (NICOLAU, 2010, p.10-11). A principal dificuldade em trabalhar analisando Q-bits em superposição emaranhados está em manter sua coerência por um tempo determinado. Visto que a descoerência acarretaria numa perca de valores, o resultado das medições num sistema quântico computacional encontrar-se-ia incerto sem o devido isolamento do mesmo. (GRECA & JUNIOR, 2013, p.19). Uma solução para conter o movimento destas partículas seria atingindo a temperatura de zero absoluto (-273,15 °C), onde as moléculas ficam sem energia cinética para movimentar-se, como é dito por Pires, Afonso & Chaves (2006):

> Pode-se imaginar que a temperatura mais baixa que pode existir é um estado térmico em que a agitação térmica, isto é, as moléculas estão em repouso. A esse limite inferior de temperatura dá-se o nome de zero absoluto. (PIRES, AFONSO & CHAVES, 2006, p.105).

4.2. CIRCUITOS QUÂNTICOS

Pesquisadores e estudiosos criaram algoritmos essenciais para a resolução de problemas utilizando o Q-bit e obtiveram soluções para cálculos matemáticos bastante complexos em segundos. Algoritmos são tarefas pré-determinadas para um sistema computar. (OLIVEIRA, 2007, p.13). De acordo com Zynger:

> Analogamente a um computador clássico, construído a partir de circuitos elétricos, fios e portas lógicas, o computador quântico será construído a partir de circuitos quânticos baseados em portas lógicas quânticas, que manipulam a informação quântica representada pelos qubits. (ZYNGER, 2015, p.18).

Apesar dos circuitos quânticos serem semelhantes aos clássicos, eles diferem muito da analogia clássica por conta de seus algoritmos e portas lógicas com

propriedades quânticas, estes que são mais rápidos que o modelo de circuitos de um computador convencional para uma mesma classe de problemas. (PORTUGAL, LAVOR, CARVALHO & MACULAN, 2004, p.14-15). Porém o problema destes circuitos encontra-se na dificuldade de desenvolvimento para tais, uma vez que o programador tenha de lidar com a complexidade de aplicar as propriedades da mecânica quântica nos algoritmos, criar um algoritmo bom e otimizado torna-se uma tarefa difícil até para tarefas simples.

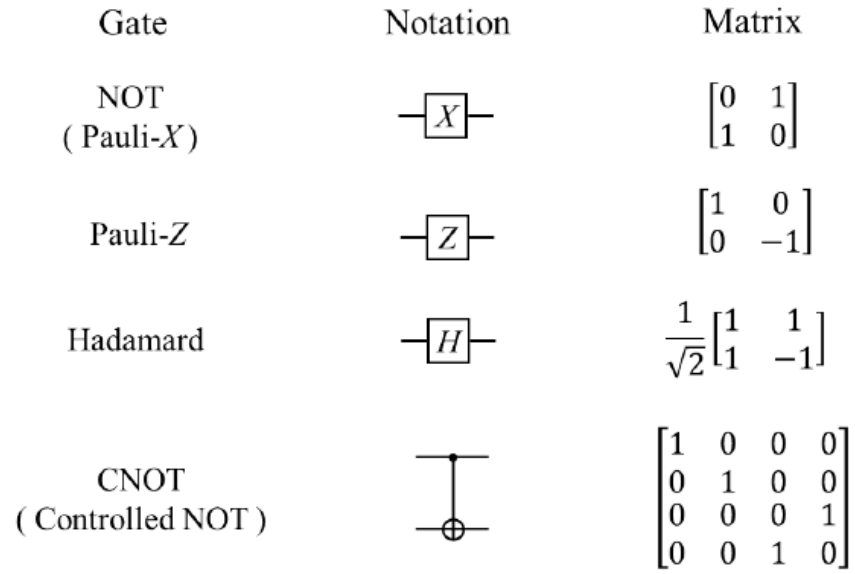


Figura 5 *– Portas quânticas mais usadas (NOT, Z, Hadamard e CNOT)*
Fonte: (researchgate.net)

4.2.1. Algoritmo de Deutsch

Em 1985, o físico israelense David Deutsch foi um grande pioneiro no campo da Computação Quântica. Deutsch propôs uma máquina que continha características da máquina universal de Turing[1], utilizando os conceitos da mecânica quântica. A principal fonte do seu poder vinha do "paralelismo quântico" (superposição de estados, emaranhamento e resultados probabilísticos das medições). Porém trabalhar com a complexa disposição dos estados é um desafio enorme para os pesquisadores. (GRECA & JUNIOR, 2013, p.17-21). Deutsch prosseguiu com os estudos de portas lógicas após a publicação de seus artigos com Richard Jozsa, criando algoritmos e identificando problemas.

[1] O matemático Alan Mathison Turing ficou conhecido como "pai da computação" após propor a criação de uma máquina automática para manipular símbolos e guardar informações. A máquina de Turing teria sido a primeira proposta do que atualmente é conhecido como computador.

Segundo Rocha, Resende & Júnior (2003), um problema bastante conhecido e identificado por Deutsch consistia na utilização de uma caixa preta que computa uma função simples de mapeamento, onde um bit $f(x)$ pode apresentar quatro possibilidades de funções, onde o bit $f(0) = f(1)$ ou $f(0) = f(0)$ e o bit $f(1) = f(1)$ ou $f(1) = f(0)$. Supondo que o cálculo da função de um bit demore 24 horas para ser resolvido, ao calcular dois bits (0 e 1) demoraria 48 horas. Logo, para discernir se a função $f(x)$ apresenta um valor constante, $f(0) = f(1)$, ou balanceada, $f(0) \neq f(1)$, não seria viável quando a solução é demandada num curto período de tempo.

O problema de Deutsch mostra que para identificar se a função é constante ou balanceada num sistema com 2 Q-bits, faz-se necessário efetuar um cálculo para cada Q-bit. Porém utilizando o princípio da superposição foi possível desenvolver um algoritmo que resolva o problema num único cálculo ao correlacionar ambos os Q-bits. Este é o benefício do paralelismo quântico, realçando ainda mais o potencial da Computação Quântica em relação com a computação clássica. (ROCHA, RESENDE & JÚNIOR, 2003, p.20-21).

4.2.2. Algoritmo de Shor

O segundo maior desafio da Computação Quântica, após manter a coerência dos Q-bits, é a de criar algoritmos que trabalhem com a complexa disposição dos estados. Em 1993 o matemático americano Peter Shor promove um dos algoritmos pioneiros na Computação Quântica sem qualquer formação na mecânica quântica. (GRECA & JUNIOR, 2013, p.19-20).

O impacto que este algoritmo causou na comunidade científica foi relativamente grande. O algoritmo de Shor mostrara-se capaz de realizar a fatoração[1] de números grandes num curto período de tempo, algo que seria impraticável com todo o aparato convencional disposto atualmente. (NICOLAU, 2010, p.1-2). Os algoritmos de fatoração são peças cruciais no tratamento da segurança de sistemas criptografados, uma vez que sua vantagem é o tempo de fatoração dos computadores casuais, e a eficiência do algoritmo de Shor num computador quântico perfeito tornaria todas as chaves de criptografias obsoletas.

[1] A fatoração é uma simplificação dos polinômios matemáticos onde as somas, subtrações ou equações são transformadas em um produto com fatores.

O segredo de seu desempenho encontra-se no paralelismo quântico. O algoritmo de Shor utiliza a mesma solução dos algoritmos de fatoração: achar o período de uma função sobre o conjunto dos inteiros. Contudo o paralelismo é utilizado para obter a representação de todos os valores de uma função em um único passo, por meio da superposição. O resultado é então calculado e apresentado em forma de porcentagem. (ROCHA, RESENDE & JÚNIOR, 2003, p.22-23).

Comprimento do número a ser fatorado (em bits)	Tempo de fatoração por algoritmo clássico	Tempo de fatoração com o algoritmo de Shor
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quatrilhões de anos	4,8 horas

Figura 6 *– Comparação entre os algoritmos clássicos e o algoritmo de Shor*
Fonte: (gta.ufrj.br)

4.2.3. Algoritmo de Grover

Em 1996 o cientista indiano Lov Grover elaborou um algoritmo de busca quântica bastante conhecido. Para realizar a busca de um elemento específico numa lista desordenada de *N* elementos demoraria o equivalente ao número de elementos disponíveis para serem testados na lista. Com o algoritmo de Grover a busca é realizada num tempo inferior, equivalente a $\sqrt{N}$. (PORTUGAL, LAVOR, CARVALHO & MACULAN, 2004, p.22).

Segundo Oliveira (2007), o algoritmo de Grover funciona em três etapas diferentes: a primeira delas é preparando os Q-bits em superposição utilizando portas Hadamard. A segunda parte consiste em marcar o elemento que deve ser encontrado através de um operador unitário chamado de “oráculo”, o oráculo marca um estado do Q-bit (0 ou 1) numa função onde $f(i)$ = 1 se o elemento for o procurado ou 0 se for o elemento errado. E a terceira etapa consiste na amplificação de amplitude, que aumenta a probabilidade de leitura do elemento marcado anteriormente.

Desta forma o algoritmo de Grover ultrapassa, também, os algoritmos clássicos de busca. A importância destes algoritmos se dá na contribuição com a expansão da Ciência da Computação Quântica. (GRECA & JUNIOR, 2013, p.20). Seja

para matemáticos, cientistas e engenheiros da computação ou pesquisadores de qualquer região do mundo. O fato é que, todos desfrutam da mesma capacidade de exercer suas pesquisas em seus determinados ramos. Atingindo conquistas e garantindo a magnificência do aparato computacional em conjunto.

5. APLICAÇÃO NO ÂMBITO CIENTÍFICO

Apesar do computador quântico poder fazer tudo o que um computador normal faz, sua utilização vai mais além nas aplicações de cunho importante em todo o parâmetro científico. Segundo a IBM (2015), existem três tipos de computadores quânticos: o *Quantum Annealer*, *Analog Quantum* e o *Universal Quantum*.

- O *Quantum Annealer* é um tipo de computador quântico de manuseio mais simples, para a otimização de problemas e que dispõe de pouco poder computacional. (IBM, 2015).
- O *Analog Quantum* se sobressai em contraste com a computação clássica por apresentar sistemas de 50 a 100 Q-bits. Sua dificuldade em manuseio é mais elevada, porém apresenta um poder computacional alto, onde emerge diversas aplicações de seu uso como, por exemplo, na Química quântica, na ciência material, na otimização de problemas, nas amostragens e nas dinâmicas quânticas. (IBM, 2015).
- O *Quantum Universal* seria o computador quântico ideal com cerca de 100 mil Q-bits físicos em seu sistema. Importante para a ciência e nos negócios, a dificuldade na construção de um computador com tais requisitos chega a ser assombrosa. Com um poder computacional muito alto, suas aplicações transcendem as do *Analog Quantum* e tornar-se-ia essencial na segurança computacional, na aprendizagem de máquinas, na criptografia e em pesquisas futuras. (IBM, 2015).

5.1. CRIPTOGRAFIA

A implicação mais evidente da Computação Quântica se dá na segurança da tecnologia. Segundo Nascimento (2014), a segurança dos sistemas atuais é ameaçada pelo avanço da Computação Quântica. Tal motivo, pois os métodos de codificação mais usados são baseados na dificuldade de fatoração de números grandes pelos computadores causais.

Este campo de estudos também revelou que a criptografia pode tornar-se ainda mais segura com os sistemas quânticos. Em 1984, os criptólogos Charles Bennett e Gilles Brassard criaram o primeiro protocolo quântico conhecido como BB84,

integrando as informações em estados quânticos e fazendo uso do paralelismo quântico. Contudo o protocolo BB84 conta com uma taxa de errônea em cerca de 25% no resultado das chaves obtidas durante as transmissões. Isto acontece, pois, o BB84 funciona com 4 estados distintos do objeto quântico (figura 7), e o receptor deve aplicar um cálculo de medição utilizando estes 4 estados aleatoriamente no objeto quântico para identificar os seus estados e encontrar uma chave. A interceptação das transmissões continua sendo possível, porém o intruso não será capaz de identificar as informações e o receptor irá notar uma invasão de acordo com o aumento no percentual da taxa de erros. Uma vez que o ato de observar influencia no objeto quântico. (UNO & FALEIROS, p.4-6).

Ainda sim este foi um dos protocolos mais bem-sucedidos e utilizados em todos os sistemas quânticos funcionais da atualidade. Com o avanço tecnológico e com implementações no campo de pesquisa criptográfica, a tendência é de melhorar as defesas e consequentemente os ataques a redes protegidas quanticamente.

A polarização de fótons pode ser usada no protocolo BB84. O fenômeno de polarização ocorre quando a luz forma ondas eletromagnéticas que vibram em direções retilíneas ou diagonais conforme a imagem retrata:

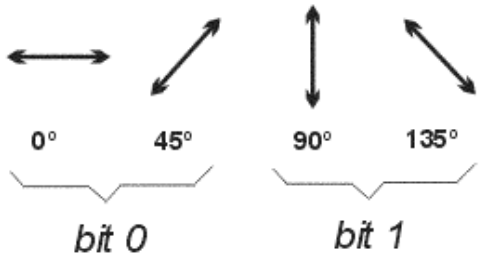


Figura 7 *– Polarizações referentes ao BB84.*
Fonte: (UNO & FALEIROS)

5.2. REDES NEURAIS

Outro ramo inspirado pela Computação Quântica é a de estudos com redes neurais artificiais, um campo da computação e informação quântica que engloba conceitos da Física moderna entrelaçados a conceitos da biologia. De acordo com Andrade, Araújo, Gomes & Fechine (2004):

> Uma rede neural pode ser vista como um modelo computacional biologicamente inspirado, que tem como principais características: a interconexão de unidades de processamento relativamente simples

> (neurônios), capacidade de aprendizagem a partir de exemplos e generalização. (ANDRADE, ARAÚJO, GOMES & FECHINE, 2004, p.1).

A chamada “Computação Natural” está tornando cada vez mais possível a semelhança entre processos biológicos com os processos computacionais. Analisar o comportamento dos seres vivos originou diversos algoritmos computacionais que servem para a resolução de problemas como otimização combinatória, agrupamento de dados, robótica coletiva, dentre outros. A expansão da Física quântica deu uma nova perspectiva aos pesquisadores que cogitavam a função do cérebro humano de “computar informações”, seu funcionamento inspirou o desenvolvimento das redes neurais artificiais. (CASTRO, CAMPELLO, HRUSCHKA & ROSATELLI, 2014, p.4).

A utilização das redes neurais também já se mostrara importante em alguns sistemas de identificação de acidentes nucleares, baseando-se em técnicas de IA (Inteligência Artificial) para fazer o diagnóstico de falhas. (NICOLAU, 2010, p.54). Segundo Vellasco (2007), as redes utilizam uma técnica estatística não-linear em elementos processadores interligados que trabalham com problemas de grande complexidade onde o ambiente de dados muda constantemente, por isso são eficientes em classificar padrões e fazer previsões. Em 1943 o psiquiatra e neuroanatomista Warren Mc Culloch e o matemático Walter Pitts desenvolveram uma máquina inspirada no cérebro humano que ocasionou no surgimento da Neuro-computação. (VELLASCO, 2007, p.3). Desde então a Computação Natural tem se tornado mais abrangente.

Os algoritmos propostos pela computação natural podem ser mais aproveitados com os sistemas quânticos, que tratam da informação com mais generalização e trabalham com resultados estimativos.

5.3. MERCADO

Por ser uma tecnologia nova, ainda apresenta limitações em suas aplicações e serventias. Segundo Grimes (2018), cerca de 44 empresas estão desenvolvendo computadores quânticos, dentre elas, a Google, IBM e Microsoft são as líderes em pesquisas. A importância de ter-se várias empresas focadas no desenvolvimento de uma tecnologia é que isto incita um mercado amplo e concorrente, de alta qualidade para o público consumidor.

A IBM já mostrou ser capaz de criar um computador quântico de 7 Q-bits para fatorar o número 15 utilizando o algoritmo de Shor[4.2.2]. (BULNES, 2005, p.87). Desde então a IBM tem aumentado o número de átomos em seus sistemas quânticos. Segundo Knight (2018), a IBM já trabalha com computadores de aproximadamente 50 Q-bits, suficiente para expor a supremacia quântica com cálculos que um computador comum não é capaz de resolver. Porém os Q-bits precisam estarem perfeitos – praticamente livres de descoerência – para operarem com confiabilidade.

Figura 8 *– Laboratório da IBM onde as máquinas quânticas estão conectadas na nuvem*
Fonte: (Technologyreview.com)

Computadores como estes são voltados inteiramente para pesquisas e contribuições científicas seja para o próprio ou para outros campos de estudo. No entanto, conforme a tecnologia é aprimorada, uma abordagem diferente vem sendo adotada. Em 2011 a empresa canadense D-Wave lançou o primeiro computador quântico no mercado. Porém há muitos questionamentos a respeito do D-Wave, uma vez que para comprovar o funcionamento perfeito de seu sistema seja uma tarefa difícil ao lidar com as propriedades da mecânica quântica. Mesmo assim empresas como a Google e a NASA já adquiriram seus computadores por um custo de aproximadamente US$ 15 milhões. (TARANTOLA, 2014).

Segundo a D-Wave (2018), o sistema de seu novo computador funciona com 2000 Q-bits. O D-Wave 2000Q™ conta com um aparelho de resfriamento que atinge cerca de -273°C (0,015 K), apresenta uma blindagem segura e lacrada em alto vácuo e consome menos energia que um computador tradicional.

Apesar de apresentar propostas duvidosas, é importante a presença de um agente ativo no mercado para incentivar as empresas que seguem com pesquisas no meio científico. Conforme os anos tudo indica que isto possa vir a tornar-se um mercado mais competitivo e importante na corrida evolucionista.

5.4. EDUCAÇÃO

A inserção da Computação Quântica na educação aconteceria mediante a introdução da Física moderna na grade curricular do Ensino Médio na matéria de Física, como exemplificação dos conceitos da mecânica quântica. Segundo Silva & Almeida (2011), a matéria de Física no Ensino Médio se restringe apenas a Física clássica. Porém os professores mostram-se cada vez mais adeptos a introduzirem o tema.

Conceitos como dualidade onda-partícula, o princípio da incerteza, superposição e estados de uma partícula poderiam ser a melhor maneira de se introduzir a Física quântica no Ensino Médio. Segundo Silva & Almeida (2011), aplicar a Física quântica traria as seguintes vantagens:

> [...] reconhecer a Física como empreendimento humano; despertar a curiosidade e entusiasmar os estudantes; apresentar aos estudantes o excitante mundo atual da pesquisa em Física; atrair jovens para a carreira científica; fato constatado em pesquisas de que a Física clássica também é alvo de sérias dificuldades conceituais por parte dos estudantes; contribuir para dar uma imagem mais correta da ciência e da natureza do trabalho científico. (OSTERMANN & MOREIRA apud SILVA & ALMEIDA, 2011, p.2-3).

Em frente a deste déficit de ensino, uma pesquisa foi realizada com uma parcela de estudantes que terminaram, que estão cursando ou que irão cursar o Ensino Médio

na cidade de João Pessoa, capital da Paraíba:

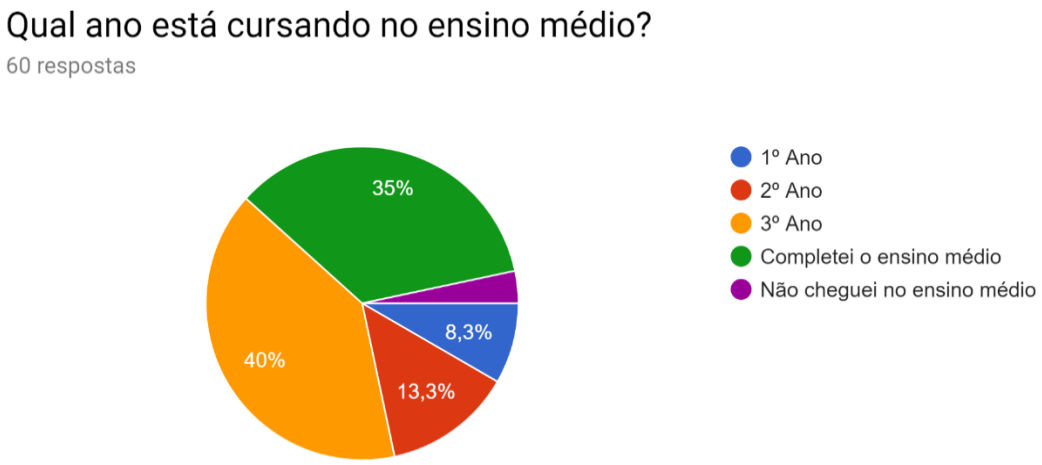


Gráfico 1 *– Qual ano está cursando*
Fonte: (próprio autor)

Diante do apresentado, nota-se que a maioria se concentra no terceiro ano do Ensino Médio. Ano em que os estudantes acumulam mais conhecimentos a respeito das disciplinas, como a Física, por exemplo. Outro gráfico revelador mostra que em toda essa quantidade de estudantes, mais da metade nunca ouviu falar sobre a Física moderna na escola:

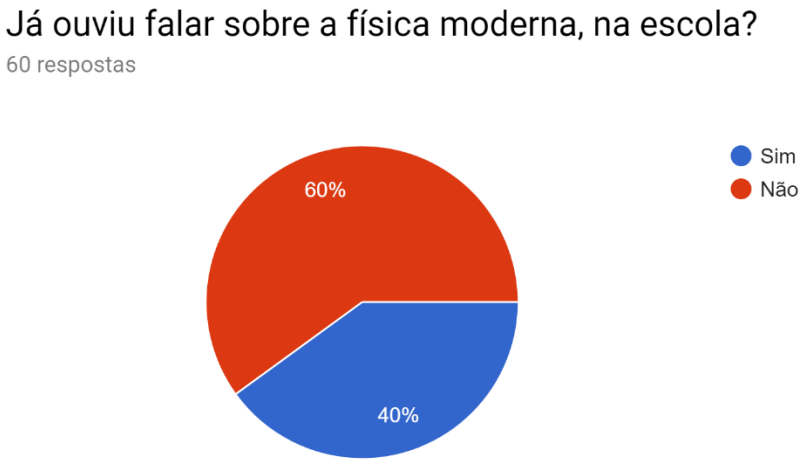


Gráfico 2 *– Já ouviu falar em Física moderna*
Fonte: (próprio autor)

E muito mais destes alunos não sabem o que é a Física moderna:

Gráfico 3 *– Sabe o que é Física moderna*
Fonte: (próprio autor)

Quando questionados a respeito da Computação Quântica no Ensino Médio, 66,7% dos estudantes já ouviram falar sobre, na escola:

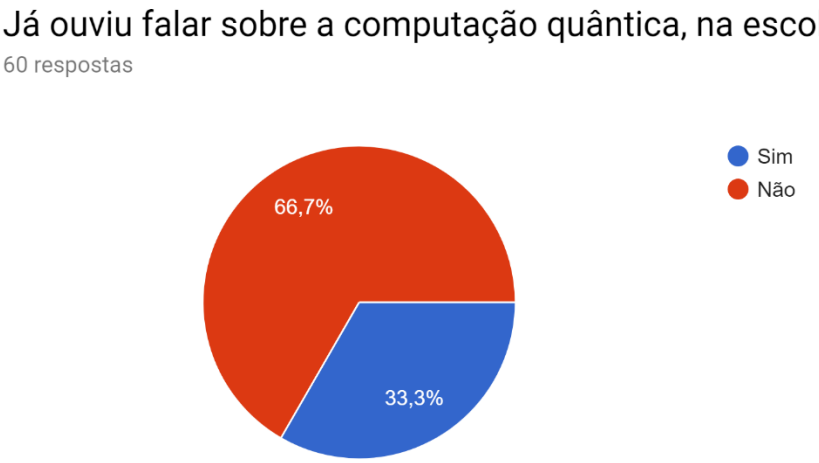


Gráfico 4 *– Já ouviu falar em Computação Quântica*
Fonte: (próprio autor)

Porém uma quantidade ainda maior não sabe o que é a Computação Quântica.

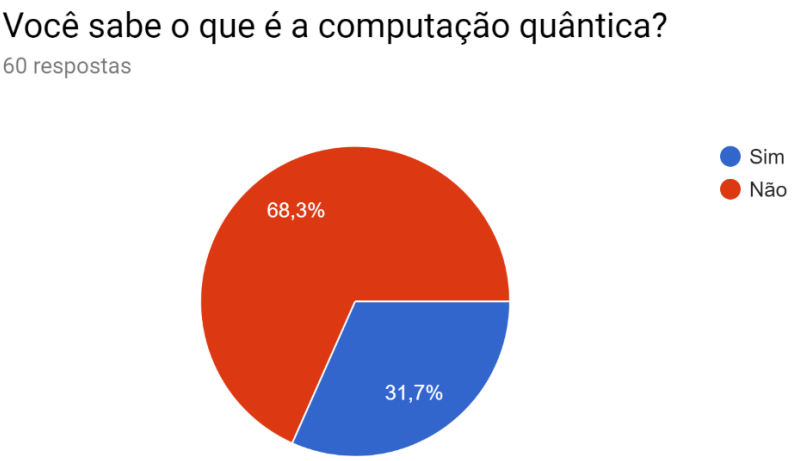


Gráfico 5 *– Sabe o que é Computação Quântica*
Fonte: (próprio autor)

E uma questão crucial que pode definir o rumo que a Física moderna pode tomar no Ensino Médio: a vontade dos estudantes de aprenderem mais sobre a área:

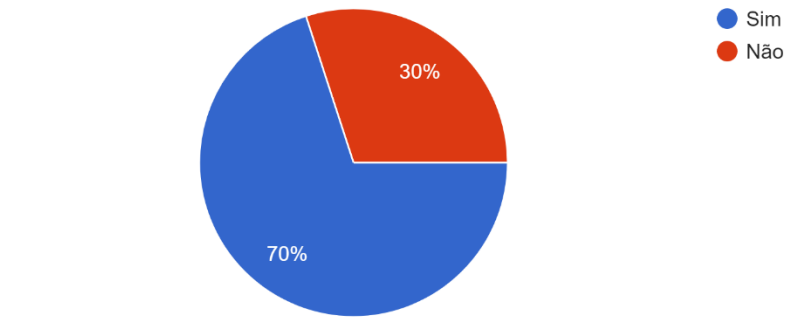


Gráfico 6 *– Quer aprender mais*
Fonte: (próprio autor)

Também foram feitas perguntas a respeito da Computação Quântica, sobre conceitos básicos abordados, e a maioria dos estudantes conseguiram lidar positivamente com as perguntas, o que mostra uma predisposição para o entendimento da ciência, até mesmo para o nível médio:

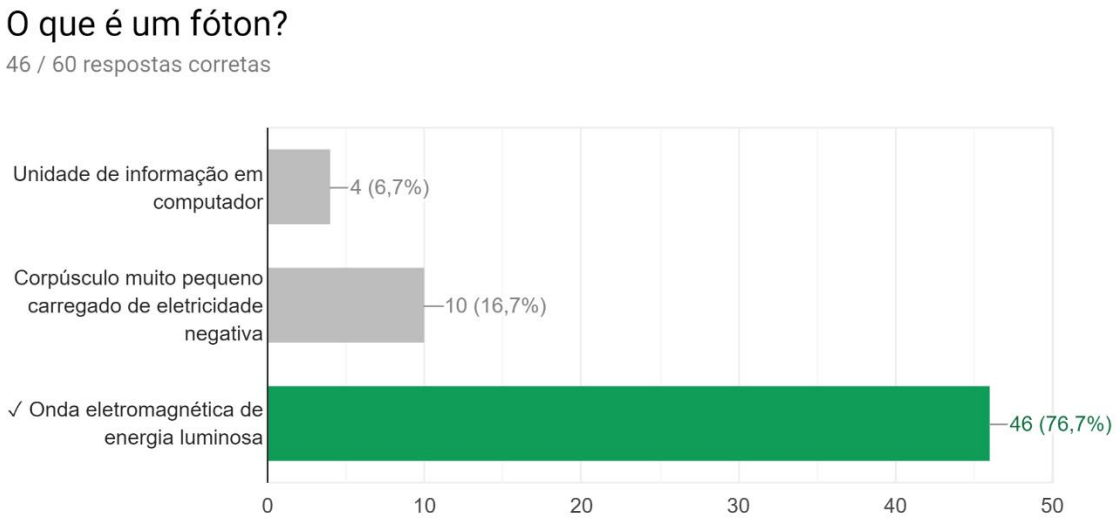


Gráfico 7 *– O que é um fóton*
Fonte: (próprio autor)

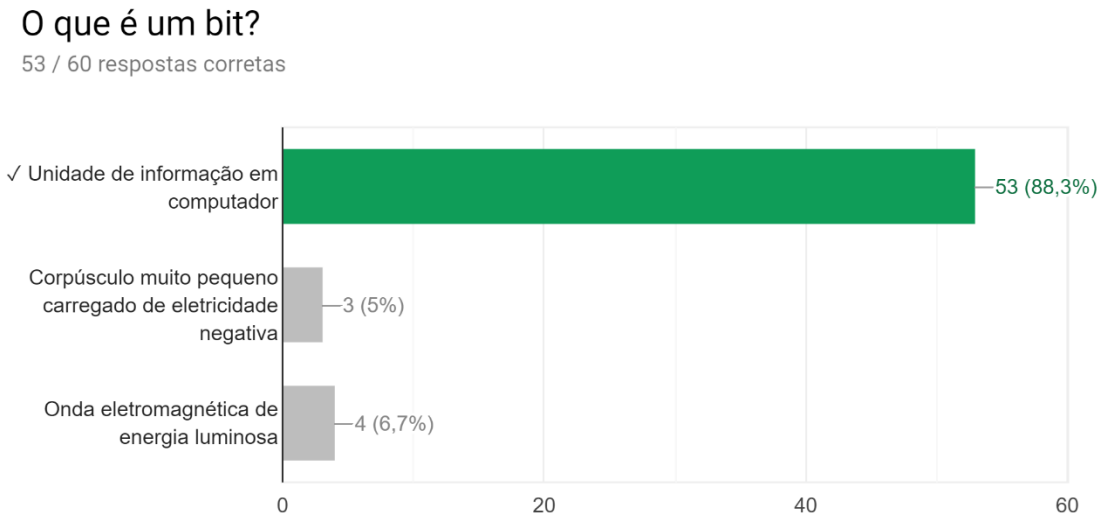


Gráfico 8 *– O que é um bit*
Fonte: (próprio autor)

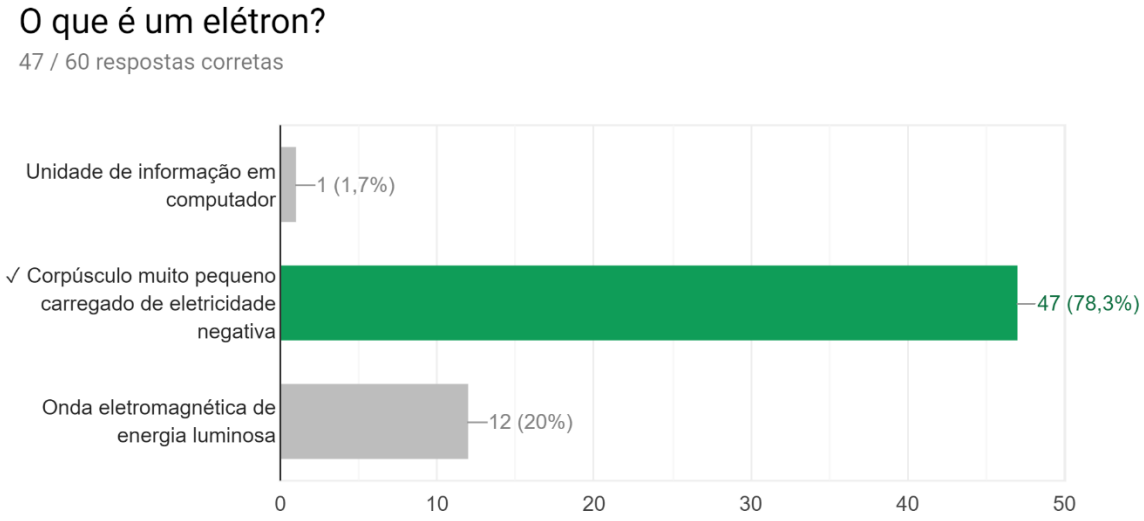


Gráfico 9 *– O que é um elétron*
Fonte: (próprio autor)

6. CONSIDERAÇÕES FINAIS

O crescente avanço tecnológico possibilitou que os grandes computadores da Segunda Guerra Mundial ficassem compactos e acessíveis ao público consumidor, por conseguinte as máquinas de computar atingiram outro patamar. A Computação Quântica compreende aspectos da Física moderna, tornando-a um campo de estudos em constante mudança devido ao mundo de incertezas que ainda assola os cientistas e pesquisadores. O princípio teórico da mecânica quântica revela aplicações práticas bastante promissoras deste aparato científico que apenas grandes empresas e alguns centros de pesquisa dispõe. A comunidade de cientistas que trabalham pela causa abrange várias partes do mundo. Oferecendo oportunidade aos diversos gêneros profissionais de contribuírem com a revolução computacional quântica.

Esta é uma área de atuação dispersa cujos resultados podem envolver e inovar outros campos de estudo do meio científico. Revolucionando áreas como a Matemática computacional, Química quântica, Física quântica, Ciência da Computação, dentre outros, fica claro a importância de se ter noção do que o ser humano está prestes a atingir. Talvez haja um futuro onde doenças complexas como o câncer possam ter uma solução a partir de algoritmos computacionais que simulam recombinações genéticas num computador quântico. O próximo passo do homem será o de dominar o mundo atômico.

O presente trabalho pauta a desinformação dos novos estudantes em relação ao campo de estudos tanto da Computação Quântica quanto da Física moderna. E ainda complementa a leitura e introduz aqueles que buscam um conhecimento mais claro e refinado da área. Apesar de ser um campo de estudos que exige muito aprofundamento aos que se propõe a contribuir, o trabalho serve como meio de inspiração para novos cientistas.

Diante do exposto, não há dúvidas de que os principais fundamentos da mecânica quântica ficaram claros mediante da complexidade reduzida do conteúdo apresentado. Os principais meios de resolução de problemas, que são os algoritmos propostos pela comunidade científica, ainda precisam de apoio para a otimização de códigos e de propostas mais inovadoras. Isto abre portas àqueles que desejam um novo cenário computacional para trabalhar e conhecer. As diversas aplicações da Computação Quântica já existentes se devem ao critério das pessoas de iniciativa que

foram capazes de criarem o cenário perfeito para a máquina atuar. Com mais anos de estudos, não há nada que impeça a tecnologia de evoluir, a exceção da convicção das novas gerações que estão por vir.

REFERÊNCIAS

AEGERTER, M.A., SIU LI, M., MUNTE, C.E., ZANATTA, A.R., 2013, "**Difração de Elétrons**", Instituto de Física de São Carlos, Universidade de São Paulo (USP) – São Paulo.

ANDRADE, W.L., ARAÚJO, B.C., GOMES, H.M., FECHINE, J.M., 2004, "**Proposta de um Neurônio Quântico**", Departamento de Sistemas e Computação, Universidade Federal de Campina Grande (UFCG) – Campina Grande.

BAKER, J., 2015, "**50 Ideias de Física quântica que Você Precisa Conhecer**", 1ed., Planeta – São Paulo.

BRENNAN, R., 2003, "**Gigantes da Física: Uma História da Física moderna Através de Oito Biografias**", Edição Revista, Zahar – Rio de Janeiro.

BRITO, A.V., "**Introdução a Arquitetura de Computadores**", 1ed, Universidade Federal da Paraíba (UFPB) – João Pessoa.

CASTRO, L.N., CAMPELLO, R.J.G.B., HRUSCHKA, E.R., ROSATELLI, M.C., "**Computação Natural: Uma Breve Visão Geral**", Programa de Mestrado em Informática, Universidade Católica de Santos (UniSantos) – Santos, São Paulo.

DECLEVA, R.S., 2012, "**Curso: Análise e Desenvolvimento de Sistemas Semestre: I. Aula 05**". Disponível em: <https://analiseedesenvolvimento.wordpress.com/?s=portas+lógicas>. Acesso em: 12/09/2018.

DUPRÉ, B., 2009, "**50 Grandes ideias da Humanidade que você Precisa Conhecer**", 1ed, Planeta do Brasil – São Paulo.

D-WAVE Systems Inc., 2018, "**The D-Wave 2000Q™ System**
The most Advanced Quantum Computer in the World". Disponível em: <https://www.dwavesys.com/d-wave-two-system>. Acesso em: 25/11/2018.

EISBERG, R., RESNICK, R., 1979, "**Física quântica: Átomos, Moléculas, Sólidos, Núcleos e Partículas**", 1ed, Elsevier – Rio de Janeiro.

EYERYS.COM, 2017, "**Google Introduces OpenFermion, A Software to Ease Scientists in Using Quantum Computers**". Disponível em: <https://www.eyerys.com/articles/news/google-introduces-openfermion-software-ease-scientists-using-quantum-computers>. Acesso em: 10/11/2018.

FÁVERO, E.M.B., 2011, "**Organização e Arquitetura de Computadores**". 1ed, Universidade Tecnológica Federal do Paraná (UTFPR) – Pato Branco.

FILHO, C.F., 2007, "**A História da Computação: O Caminho do Pensamento e da Tecnologia**", 1ed, EDIPUCRS – Porto Alegre.

FREIRE JR.O., PESSOA JR.O., BROMBERG, J., 2011, "**Teoria Quântica: Estudos Históricos e Implicações Culturais**", Livraria da Física – São Paulo.

FUTURETIMELINE.NET, 2015, "**A Breakthrough in Replacing Silicon with Carbon Nanotubes**". Disponível em: <https://www.futuretimeline.net/blog/2015/10/3-2.htm>. Acesso em: 20/09/2018.

GERHARDT, T.E., SILVEIRA, D.T., 2009, "**Métodos de Pesquisa**", 1ed, Universidade Federal do Rio Grande do Sul (UFRGS) – Rio Grande do Sul.

GRECA, I.M., HERSCOVITZ, V.E., 2005, "**Superposição Linear em Ensino de Mecânica Quântica**", Instituto de Física, Universidade do Rio Grande do Sul (UFRGS) – Porto Alegre.

GRECA, I.M., JUNIOR O.F., 2013, "**Informação e Teoria Quântica**", Sientae Studia Vol. 11, No. 1, Departamento de Filosofia, Universidade de São Paulo (USP) – São Paulo.

GRIMES, R., "**Como Computadores Quânticos Irão Destruir e (Talvez) Salvar a Criptografia**", Disponível em: <http://cio.com.br/tecnologia/2018/08/02/como-computadores-quanticos-irao-destruir-e-talvez-salvar-a-criptografia/>. Acesso em: 01/09/2018.

IBM RESEARCH. 2015, "**Infographic: Three Types of Quantum Computing**", Disponível em: <https://www-03.ibm.com/press/us/en/pressrelease/48258.wss>. Acesso em: 20/11/2018.

KNIGHT, W., 2018, "**Serious Quantum Computers Are Finally Here. What Are We Going to Do with Them?**". Disponível em: <https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/>. Acesso em: 25/11/2018.

KON, F., 2016, "**Introdução a Ciência da Computação com Python**", Curso ministrado pelo Prof. KON, F., Departamento de Ciência da Computação da USP. Disponível em: <https://www.youtube.com/watch?v=rh65Lh5V7S0>. Acesso em: 04/10/2018.

LOPEZ, F.D., CARAPETO, L.A.V., LIMA, V.F.O., "**Redes de Computadores 1: Criptografia Quântica**". Disponível em: <https://www.gta.ufrj.br/grad/10_1/quantica/quantica.pdf>. Acesso em: 15/11/2018.

MARCONI, M.A., LAKATOS, E.M., 2003, "**Fundamentos de Metodologia Científica**", 5ed, Atlas – São Paulo.

MATTIELO, F., SILVA, G.G., AMORIM, R.G., SILVA, W.B., 2012, "**Decifrando a Computação Quântica**", Caderno de Física da Universidade Estadual de Feira de Santana (UEFS) 10 (01 e 02) – Bahia.

MEHL, E., "**Do Transistor ao Microprocessador**", Engenharia Elétrica e Sociedade I: Texto sobre a História da Eletrônica, Mestre e Doutor em Engenharia Elétrica, Universidade Federal do Paraná (UFPR), Brasil.

MELLO, U., "**Como a Computação Quântica Promete Revolucionar Nosso Conhecimento**", Disponível em: <http://idgnow.com.br/ti-corporativa/2018/05/06/como-a-computacao-quantica-promete-revolucionar-nosso-conhecimento/>. Acesso em: 11/08/2018.

NASCIMENTO, M.P., 2014, "**Criptografia Quântica: Novas Tecnologias na Segurança de Dados e Telecomunicações**", Instituto Municipal de Ensino Superior de Assis (IMESA) – Assis.

NICOLAU, A.S., 2010, "**Computação Quântica e Inteligência de Enxames Aplicados na Identificação de Acidentes de uma Usina Nuclear PWR**", Dissertação de Mestrado em Ciências em Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro.

NOVAES, M., STUDART, N., 2016, "**Mecânica Quântica Básica**", 1ed., Livraria da Física – São Paulo.

OLIVEIRA, N.A., 2007, "**A Utilização do Algoritmo Quântico de Busca em Problemas da Teoria da Informação**", Dissertação de Mestrado, Centro de Engenharia Elétrica e Informática, Universidade Federal de Campina Grande (UFCG) – Campina Grande.

OLIVEIRA, I.S., 2009, "**Física moderna para Iniciados, Interessados e Aficionados**", Vol. 2., Livraria da Física – São Paulo.

OLIVEIRA, I.S., SARTHOUR, R.S., 2004, "**Computação Quântica e Informação Quântica**", 1ed., Centro Brasileiro de Pesquisas Físicas, Escola do CBPF – Rio de Janeiro.

PIRES, D.P.L., AFONSO, J.C., CHAVES, F.A.B., 2006, "**A Termometria nos Séculos XIX e XX**", Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro.

PORTUGAL, R., LAVOR, C.C., CARVALHO, L.M., MACULAN, N., 2004, "**Uma Introdução aos Algoritmos Quânticos**", Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro.

PORTUGAL, R., LAVOR, C.C., CARVALHO L.M., MACULAN N., 2004, "**Notas em Matemática Aplicada; 8: Uma Introdução à Computação Quântica**", 2ed., Sociedade Brasileira de Matemática Aplicada e Computacional – Vitória, ES.

ROCHA, A.R., RESENDE, A.M.P., JÚNIOR, A.T.C., 2003, "**Desenvolvimento de um Simulador de Algoritmos Quânticos Utilizando a Computação Convencional**", Universidade Federal de Lavras (UFLA) – Lavras.

ROSA, P.S., 2004, "**Louis de Broglie e as Ondas de Matéria**", Tese de Mestrado, Instituto de Física, Universidade Estadual de Campinas (UEC) – Campinas, São Paulo.

RUSSON, M., 2017, "**Computação Quântica: Como Será a Internet Super-rápida do Futuro**", Disponível em: <https://www.bbc.com/portuguese/geral-41697094>. Acesso em: 06/08/2018.

SAINT-EXUPÉRY, A., 2000, "**O Pequeno Príncipe**", 1ed, Agir – França

SILVA, A.C., ALMEIDA, M.J.P.M., 2011, "**Física quântica no Ensino Médio: O Que Dizem as Pesquisas**", Universidade Faculdade de Educação (Unicamp) – Campinas.

TARANTOLA, A., 2014, "**Baseado em Teoria Quântica, D-Wave 2 pode Ser Mais Rápido que um Supercomputador**". Disponível em: <https://gizmodo.uol.com.br/d-wave-2-quantico>. Acesso em: 25/11/2018.

UNO, D.N., FALEIROS, A.C., "**Princípios de Criptografia Quântica**", Instituto Tecnológico de Aeronáutica – São Paulo.

VELLASCO, M.M.B.R., 2007, "**Redes Neurais Artificiais**", Pontifícia Universidade Católica do Rio de Janeiro (PUC) – Rio de Janeiro.

WIKIPEDIA.ORG, 2008, "**Gato de Schrödinger**". Disponível em: <https://pt.wikipedia.org/wiki/Gato_de_Schrödinger>. Acesso em: 07/10/2018.

YAN, F., ILIYASU, A.M., JIANG, Z., 2014, "**Quantum Computation-Based Image Representation, Processing Operations and Their Applications**". Disponível em: <https://www.researchgate.net/publication/266855738_Quantum_Computation-

Based_Image_Representation_Processing_Operations_and_Their_Applications>. Acesso em: 13/11/2018.

ZYNGER, J., 2015, "**Algoritmo Quântico para Equações Lineares**", Instituto de Matemática, Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro.