CENTRO EDUCACIONAL FUNDAÇÃO SALVADOR ARENA

FACULDADE DE TECNOLOGIA TERMOMECANICA

LUCAS BOULLE FIGUEIREDO

DAVID CONDE DE SOUSA

LEONARDO RIBEIRO ARAGÃO

FILIPE MARQUES DE LIMA

IAGO GOMES MACEDO

**COMPUTAÇÃO QUÂNTICA**

APLICAÇÕES PARA CIÊNCIA E RESISTÊNCIA DOS MATERIAIS

São Bernardo do Campo

2018

LUCAS BOULLE FIGUEIREDO

DAVID CONDE DE SOUSA

LEONARDO RIBEIRO ARAGÃO

FILIPE MARQUES DE LIMA

IAGO GOMES MACEDO

**COMPUTAÇÃO QUÂNTICA**

APLICAÇÕES PARA CIÊNCIA E RESISTÊNCIA DOS MATERIAIS

Trabalho de N1, apresentado à disciplina ciência e resistência dos materiais, do curso de engenharia da computação da Faculdade de Tecnologia Termomecanica, como requisito parcial para a obtenção do título de Bacharel.

Orientador: Prof. Dr. Márcio Silva

São Bernardo do Campo

2018

**RESUMO**

A área da computação caracteriza-se como volátil e altamente regenerativa no seu sentido de aprimoramento e estruturação, ao passo de seu desenvolvimento e tendências, este trabalho tem como objetivo revisar a temática envolvida na área de pesquisas acerca da computação aplicada na área quântica, sobretudo aos seus aspectos coercitivos, e ao mesmo tempo implementadores das atuais abordagens sobre a tecnologia e seus possíveis usos. Os temas desse estudo envolvem itens como; fundamentos da mecânica quântica, sua breve história e surgimento, materiais utilizados em sua construção, fabricantes atuantes no mercado, tendências para aplicação e seu impacto no atual conceito da tecnologia. Atualmente seu uso é limitado a capacidade de execução devido à dificuldade da aplicação teórica na física e seus critérios de incertezas, assim como a necessidade comportamental dos materiais próximo ao conceito de perfeição e simetria, além do desconhecimento e abstração do seu próprio funcionamento.

**ABSTRACT**

Computational area is characterized as volatile and highly regenerative in its sense of improvement and structuring. This work has objective to review researches involved in computation, applied in the quantum area, mainly its coercive aspects, at the same time implementers of current approaches to technology and its possible uses. Themes of study involve items such as; fundamentals of quantum mechanics, its brief history and emergence, materials used in its construction, manufacturers in market, trends for application and impacts on the current concept of technology. Nowadays, its use is limited to the execution capacity due to the difficulty of the theoretical application in physics and criteria of uncertainties, as well as the behavioral need of the materials close to the concept of perfection and symmetry, besides the ignorance and abstraction of its own functioning.

**LISTA DE FIGURAS**

|  |  |
| --- | --- |
| Figura 1 –Experimento de dupla fenda de Thomas Young................................ | 12 |
| Figura 2 –Ilustração do efeito fotoelétrico............................................................ | 14 |
| Figura 3 – Quantidade de transistores em chips e Velocidade de processamento | 20 |
| Figura 4 – Evolução das máquinas com as décadas.......................................... | 21 |
| Figura 5 – Bristlecone, o novo processador quântico da Google........................ | 26 |
| Figura 6 – Rodada 0 em algoritmo de busca paralela......................................... | 30 |
| Figura 7 – Rodada 1 em algoritmo de busca paralela......................................... | 30 |
| Figura 8 – Rodada 2 em algoritmo de busca paralela......................................... | 31 |
| Figura 9 – Rodada 3 em algoritmo de busca paralela........................................ | 31 |
| Figura 10 – Rodada final em algoritmo de busca paralela.................................. | 32 |
| Figura 11 – David P. DiVincenzo.......................................................................... | 34 |
| Figura 12 – Cientista Observando Átomo sobre aprisionamento......................... | 36 |
| Figura 13 – Laboratório de resfriamento a lazer e aprisionamento NIST............ | 36 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**LISTA DE TABELAS**

|  |  |
| --- | --- |
| Tabela 1 - Números codificados na lista de nomes............................................. | 29 |
| Tabela 2 - Grupos do INCT-IQ.............................................................................. | 40 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**SUMÁRIO**

[1 - INTRODUÇÃO 9](#_Toc524648960)

[1.1 Delimitação do tema 9](#_Toc524648961)

[1.2 Problemas e premissas 9](#_Toc524648962)

[2. A História da Mecânica Quântica 11](#_Toc524648963)

[2.1 Efeito Fotoelétrico 11](#_Toc524648964)

[2.1.1 Motivação Histórica 11](#_Toc524648965)

[2.1.2 Teorias de Einstein para o Efeito Fotoelétrico 13](#_Toc524648966)

[2.2 Dualidade Onda-Corpúsculo 14](#_Toc524648967)

[2.3 Princípio de Incerteza de Heisenberg 15](#_Toc524648968)

[2.3.1 Versão ontológica 15](#_Toc524648969)

[2.3.2 Versão epistemológica 16](#_Toc524648970)

[2.4 Funções de Onda 17](#_Toc524648971)

[2.5 Espaço de Hilbert 17](#_Toc524648972)

[2.6 Superposição 18](#_Toc524648973)

[2.7 Emaranhamento (entanglement) 18](#_Toc524648974)

[3. O INICIO DA COMPUTAÇÃO QUÂNTICA 19](#_Toc524648975)

[3.1 Lei de Moore 19](#_Toc524648976)

[3.2 Experiência com fótons 23](#_Toc524648977)

[3.3 Primeiros avanços 24](#_Toc524648978)

[3.4 Manipulação de dados e erros quânticos 24](#_Toc524648979)

[3.5 Primeiras maquinas 25](#_Toc524648980)

[2.5.1. IBM 25](#_Toc524648981)

[2.5.2. Computador híbrido 26](#_Toc524648982)

[4 CONCEITOS DA MECÂNICA NA COMPUTAÇÃO QUÂNTICA 27](#_Toc524648983)

[4.1 Codificação densa 27](#_Toc524648984)

[4.2 Teorema no-cloning 27](#_Toc524648985)

[5 ALGORITMOS PARA COMPUTADORES QUÂNTICOS 28](#_Toc524648986)

[6 COMPUTAÇÃO QUÂNTICA E SOCIEDADE: COMO TORNAR REAL A COMPUTAÇÃO QUÂNTICA? 34](#_Toc524648987)

[6.1 A forma do qubit 34](#_Toc524648988)

[6.2 O estado inicial do qubit 35](#_Toc524648989)

[6.3 Tempo de Decorrência 37](#_Toc524648990)

[6.4 Portas Lógicas 38](#_Toc524648991)

[6.5 Leitura do Qubit 38](#_Toc524648992)

[6.6 Computação Quântica no Brasil 39](#_Toc524648993)

**CONCLUSÃO**…………………………………………………………………..…………. 41

[**REFERÊNCIAS** 40](#_Toc524648994)3

# 1 – INTRODUÇÃO

## 1.1 Delimitação do tema

Trabalha-se em torno da introdução ao ferramental teórico da mecânica quântica, para compreensão de como pode funcionar uma máquina que vai além da transformação de picos de energia elétrica em sinais. Trata-se dos principais pontos da mecânica quântica que tem influência direta no funcionamento de computadores quânticos, sem aprofundá-los matemática ou teoricamente.

Além disso, cabe a discussão das aplicações e efeitos dos processadores quânticos para as áreas atuais da tecnologia da informação, além de buscar incentivar o leitor a partir de um olhar crítico para a tecnologia em desenvolvimento

refletir sobre seus possíveis potenciais transformadores em uma sociedade de relações tão complexas e onde a tecnologia tem um papel tão crucial.

Entende-se ainda que a ferramenta matemática necessária para uma compreensão mais profunda do tema em questão é desnecessária no contexto atual dada a natureza introdutória deste material.

## 1.2 Problemas e premissas

O assunto em questão é intrinsecamente relacionado a física quântica, área da física que lida com as interações das partículas subatômicas e com dados probabilísticos e em sua maioria experimentais, o que a torna instável, além de ainda estar longe de ser um tema tão bem conhecido e estudado como a mecânica de Newton ou o Eletromagnetismo de Faraday e Lenz. Sendo assim, a física quântica, e no caso da computação quântica, especificamente a mecânica quântica tem sofrido revoluções e questionamentos desde o momento de seu surgimento, ocasionando a dificuldade de predição de comportamentos a partir de uma base teórica sólida, apesar da existência do modelo padrão.

Por se tratar de um tema novo e em expansão, as análises quanto a suas aplicações e potenciais são baseadas em estudos de caso superficiais de empresas como a Google e a IBM e suas máquinas atuais.

Quando surgiu a computação quântica? Onde surgiu? Quais problemas esta se propõe a resolver? Quem é/foi o expoente da computação quântica? Quais suas aplicações práticas? Quais os usos atuais e a quais necessidades de nossa sociedade ela atende? Será a computação quântica algum dia tão comum quanto a computação que temos hoje ou isso seria inviável?

Essas são algumas das perguntas que, de maneira breve e em termos gerais, procura-se responder através destas páginas.

# 2. A História da Mecânica Quântica

O mundo foi tomado por novas tecnologias que estão em constante mudança. As placas mães, os processadores, cada parte da tecnologia é melhorada quando menor e é aí que a física moderna revoluciona nossa sociedade, seu objeto de estudo é o que não podia antes ser visto, é o que só recentemente está sendo descoberto e entendido, o universo micro, nano, pico e o comportamento das partículas nesses universos.

Até o fim do século XIX, a mecânica clássica juntamente com o termodinâmica e o eletromagnetismo formavam a linha de frente dos estudos físicos, entretanto, no início do século XX, três problemas principais que não puderam ser descritos pelas ferramentas teóricas da física contemporânea impulsionaram os estudos desta época e revolucionaram a física: o efeito fotoelétrico, a radiação espectral do hidrogênio e a radiação de corpo negro, como descrito por Gil da Costa Marques e Maria José Bechara, 2007.

A mecânica quântica então começa a caminhar a partir da formulação de Max Planck (uma das maiores referências em estudos de mecânica quântica) formulando as leis da radiação do corpo negro; seguido por Einstein resolvendo o efeito fotoelétrico, além da sua famigerada Teoria da Relatividade que revolucionou a mecânica; tem-se também a lei de Stefan-Boltzmann e a série de Balmer, todas resoluções para os problemas elementares da física quântica.

### 2.1 Efeito Fotoelétrico

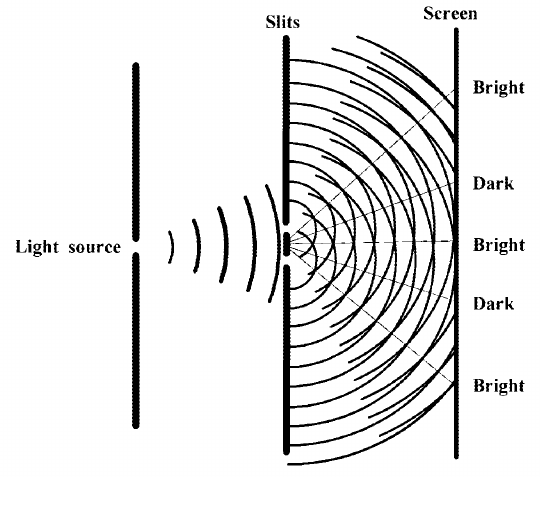
### 

### 2.1.1 Motivação Histórica

O pontapé inicial para a compreensão da luz foi com a concepção de Heron de Alexandria que a luz caminhava em linha reta e foi somente em 1621 que o matemático Wilbord Snell foi capaz de explicar este fenômeno, constatando que a diferença entre a angulação dos raios de luz era dada pela refração do meio em que penetravam continuando em linha reta.

A partir disso, as discussões passaram a estar ao em torno da incerteza da luz ter uma natureza ondulatória ou corpuscular, envolvendo grandes nomes como Isaac Newton e seus experimentos com os prismas, e Thomas Young, nome conhecido por seu experimento de dupla fenda[1] que inicialmente trouxe um consenso a academia de que a luz se propagava como uma onda.

**Figura 1: experimento de dupla fenda de Thomas Young**



A partir do entendimento de que a luz teria um comportamento ondulatório e com a teoria de Maxwell sobre a luz ser uma onda eletromagnética (Maxwell, 1864), podia-se então produzir outros tipos de ondas eletromagnéticas a partir de circuitos elétricos assim como fez Heinrich Hertz.

Durante as suas experiências, Hertz notou que a luz produzida por uma faísca num circuito podia induzir uma corrente elétrica em outros circuitos afastados, que empregava para detectar as ondas eletromagnéticas. Alguns anos depois, com a descoberta do elétron por parte de Thomson, ficou claro que o efeito observado por Hertz, designado de Efeito Fotoelétrico, era devido ao escape de alguns eletrões em um metal, quando era atingido por luz. (SILVA, 2006)

Uma vez definido o efeito fotoelétrico a problemática era o fato da energia dos elétrons não aumentar conforme a intensidade da luz era aumentada, mas sim em função da frequência que incidia sobre o metal e a teoria ondulatória clássica da luz não era capaz de explicar tal fato. São três os fatores que impediam a teoria clássica de ser suficiente para explicar tal problemática:

1) A teoria ondulatória requer que o vetor campo elétrico oscilando, *E*, da onda de luz aumente em amplitude conforme a intensidade do feixe de luz é aumentado. [...]. Entretanto, a energia cinética máxima, que é igual a eV0, independe da intensidade da luz. Esse resultado tem sido testado ao longo de uma faixa de intensidades de 107.

2) De acordo com a teoria ondulatória, o Efeito Fotoelétrico poderia ocorrer para qualquer frequência da luz, desde que aquela luz fosse intensa o bastante para dar a energia necessária para ejetar os fotoelétrons. [...]. Por outro lado [...]. Para frequências inferiores a v0 o Efeito Fotoelétrico não ocorre.

3) [...] Na Teoria Clássica, a energia da luz é uniformemente distribuída sobre a frente de onda. Por isso, se a luz é fraca o bastante, deveria haver um atraso no tempo mensurável [...]. Durante esse intervalo, o elétron deveria estar absorvendo energia de um feixe, até que ele tivesse acumulado o bastante para escapar. No entanto, nenhuma defasagem de tempo detectável foi, jamais, medida. (SILVA, 2006)

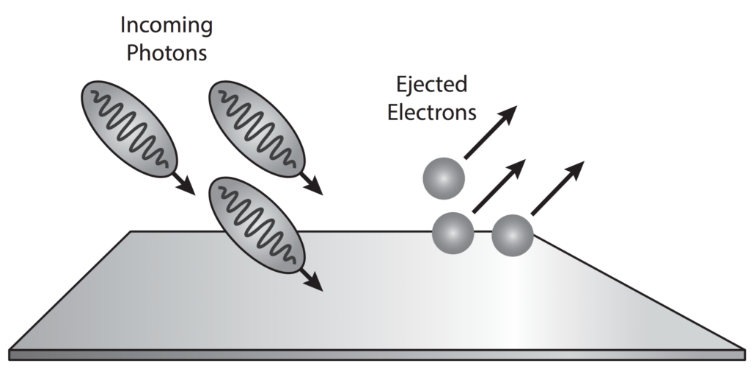
Havia uma certeza e um entendimento empírico profundo em relação a maneira como a luz se propagava, e teoria eletromagnética era suficiente para explicar tal fenômeno, entretanto, não era capaz de explicar a emissão e absorção da luz; foi então que Albert Einstein revoluciona a física ao explicar o funcionamento do efeito fotoelétrico, sendo recompensado com um Prêmio Nobel.

### 2.1.2 Teorias de Einstein para o Efeito Fotoelétrico

Einstein compreende o efeito fotoelétrico a partir de “pacotes” de energia, ideia anteriormente proposta por Planck para resolver um outro problema.

Einstein raciocinou da seguinte forma: a exigência de Planck que a energia contida nas ondas eletromagnéticas de frequência *v* na fonte irradiante (exemplo: uma fonte de luz ultravioleta em um experimento fotoelétrico) podia ser somente 0, ou h*v*, ou 2h*v*, ou nh*v*, implicava que, no processo de passagem do estado de energia nh*v* para o estado de energia (n - 1) hv. Haveria uma emissão discreta de energia eletromagnética da energia h*v*. (SILVA, 2006)

**Figura 2: ilustração do efeito fotoelétrico**



Cada elétron, portanto, absorve somente um “pacote” de energia de cada vez. Essas quantidades foram chamadas por Planck de quanta, e tem sido nomeada de fótons. Einstein compreende que esses fótons se movimentam como ondas, mas sua posição final é dada com uma natureza corpuscular, observações feitas a partir do experimento de dupla fenda. Formulou então que a energia cinética de um fóton é sua energia menos seu trabalho:

*K = h*v *– W (1)*

Analogamente, Einstein conseguiu definir que a energia cinética máxima é a subtração da energia de um fóton pela função trabalho (que é a energia mínima necessária para que um elétron escape da superfície do metal):

*K = h*v *– w0 (2)*

## 

## 2.2 Dualidade Onda-Corpúsculo

A primeira evidência do caráter dual da luz foi observada pelo físico russo Pyotr

Nikolayevich Lebedev (1866-1912) ao realizar experiências sobre a pressão exercida pela luz sobre os corpos, mas a primeira relação formal só foi feita por Albert Einstein 20 anos depois.

"Com efeito, ele [Einstein] demonstrou que: h ν = hc/λ = mc2 = pc → p = h/λ. Aí está, portanto, o caráter dual da luz, já que as características ondulatórias (λ) e corpuscular (p) não são independentes." (Bassalo e Farias, 2016)

Mais adiante, de Broglie postula a ideia de "ondas de matéria", aonde todas as partículas se comportariam como ondas, em maior ou menor escala.

## 2.3 Princípio de Incerteza de Heisenberg

O princípio de incerteza de Heisenberg é obtido pelo físico de mesmo sobrenome a partir da expansão do conceito já existente na mecânica quântica a época de suas observações (fim da década de 1920): não se podia medir com precisão a posição e o momentum com valores numéricos ao mesmo tempo e também do postulado quântico de Bohr (Chibeni apud Bohr, 1928).

De maneira geral, Heisenberg buscou explicar as discrepâncias internas presentes na já aceita, porém cheia de inconsistências, teoria quântica.

Os argumentos utilizados por Heisenberg podem ser divididos entre o ontológico: que trata do ser e o epistemológico: que trata do nosso conhecimento.

### 2.3.1 Versão ontológica

A argumentação de Heisenberg parte da teoria de Louis de Broglie posteriormente tratada quanticamente por Schrödinger: todos os objetos quânticos podem ser representados por "pacotes de onda", dada a já citada natureza ondulatória e corpuscular da matéria, não se faz necessário refletir sobre os possíveis impactos da teoria de Schrödinger.

δx δp ≥ h/2π (3)

Essa é a relação de Heisenberg para posição e momentum obtida a partir de observações da relação entre pacotes de onda no espaço de coordenadas (x) e no espaço dos números de onda (k), juntamente com o postulado de Broglie.

[...] se trata aqui de um limite na possibilidade de se definirem de modo preciso algumas das propriedades dinâmicas dos objetos. Na abordagem adotada esses objetos seriam, como já foi dito, entes ondulatórios, de modo que é fácil perceber que não possuem em si próprios uma posição e uma velocidade bem definidas. [...]. Parece, pois, adequado classificar a presente versão das relações de ontológica: ela diria respeito a uma indeterminação intrínseca aos entes físicos. (Chibeni, 2004)

Entende-se que não seria possível existir o momentum e a posição simultaneamente com valores bem definidos, sendo isto característica própria de qualquer ente físico. Por isso a nomenclatura de "ontológica", sendo esta parte da natureza do ser.

### 2.3.2 Versão epistemológica

Esta é a versão pela qual se estabelece o nome de princípio da incerteza. Heisenberg afirma que para que se possa fazer inferir algo a partir de uma afirmação "é preciso especificar experimentos definidos com o auxílio dos quais se pretenda medir a ‘posição do elétron’; caso contrário, a expressão não terá nenhum significado. "(Chibeni apud Heisenberg, 1927 p. 64).

Logo, somente um experimento por meio do qual se estabeleça a aplicação do conceito ou se possa atribuir um valor numérico preciso conferem legitimidade a um conceito.

Nessa seção, o raciocínio considerado é o de que cada objeto que se procura observar é uma partícula e tem momento e posição bem definidos, porém partindo desde o princípio da imprecisão da medida no experimento feito por Heisenberg e sabido que as grandezas não poderão ser determinadas experimentalmente com alta precisão, o raciocínio inicial cai por terra.

Nesta versão, e somente nela, a denominação usual de “princípio da incerteza” é justificada. Ora, incerteza é uma noção epistêmica, ou seja, relativa ao nosso conhecimento. Nesta versão, as relações de Heisenberg não expressariam, pois, uma característica física dos objetos (com na versão precedente), mas uma característica de nosso conhecimento acerca dos objetos. (Chibeni, 2004)

As relações de Heisenberg, portanto, mostra como evitar conflitos de conceitos e demonstra os limites nos quais a concepção de partícula pode ser aplicada.

## 2.4 Funções de Onda

As funções de onda são representações matemáticas abstratas do estado de um sistema, descrevendo todos os possíveis estados de um sistema. A função de onda é uma amostra de como o princípio da incerteza é a realidade nos estudos da mecânica quântica.

## 2.5 Espaço de Hilbert

Continuamos a trabalhar com conceitos que regem a mecânica quântica, especificamente trataremos de agora em diante de conceitos mínimos necessários para compreensão desta pesquisa.

Um espaço de Hilbert é um espaço vetorial completo normado, sendo este um espaço de Banach com um produto interno. Este possui infinitas dimensões e utiliza o corpo dos números complexos. Tanto as funções de onda quanto a transformada de Fourier possui sua representação máxima e natural no espaço de Hilbert.

## 

## 2.6 Superposição

A superposição é a compreensão da sobreposição de possíveis estados para um mesmo sistema como descrito a partir das funções de onda.

"Seguindo a nomenclatura de Hughes, dados dois estados puros | pi › e | pj › tais que, para dois resultados diferentes xi e xj , pi(xi) = 1 (a probabilidade de, para o estado | pi › , se obter o valor xi , é igual a 1) e pj(xj) = 1 (a probabilidade de, para o estado | pj ›, se obter o valor xj , é igual a 1), pode-se construir um outro estado puro | pk › em MQ tal que para qualquer resultado xn (n = i ou j) do experimento em questão, pk(xn) = cipi(xn) + cjpj(xn), onde 1 0 ≤ ci ≤ , 0 ≤ cj ≤ 1 e ci + cj = 1. Então, 0 ≤ pk(xi) = ci ≤ 1. Rompe-se desta forma a identidade que a Física Clássica estabelece entre estado de um sistema e resultado de uma medição, ou seja, o resultado de uma medição não informa de forma completa sobre o estado do sistema antes da medida, ocorrendo apenas relações em forma probabilística." (Greca e Herscovitz, 2005)

É na tentativa de explicar esse princípio que Schrödinger formularia o paradoxo do gato (um *Gedankenexperiment* - experimento imaginário), onde o gato poderia estar tanto vivo quanto morto dependendo da desintegração de um átomo que *poderia ou não ocorrer*, ou seja, o estado atual do gato nada mais seria do que a combinação de todos os possíveis estados que ele teria dado a natureza incerta do fato. Com o passar do tempo e o avanço dos estudos, os limites para até aonde a mecânica quântica poderia descrever os fenômenos (micro/macro) ficou mais claro o paradoxo de Schrödinger se torna apenas uma ilustração didática para compreensão do fenômeno da superposição.

O efeito em questão se tornou o principal expoente da computação quântica a partir do momento em que em 1996, um grupo de cientistas do *National Institute of Standards and Technology*, Colorado, Estados Unidos, conseguiu criar "gatos de Schrödinger" com elétrons e átomos, fazendo com que estes estivessem em dois lugares ao mesmo tempo, o que possibilita a computação quântica.

## 2.7 Emaranhamento (*entanglement*)

De maneira geral, o emaranhamento é uma consequência do princípio da superposição quando falamos de dois ou mais subsistemas. O emaranhamento tem influência direta dentro da Teoria Quântica da Informação na codificação superdensa e no teletransporte quântico.

# 3. O INICIO DA COMPUTAÇÃO QUÂNTICA

A computação quântica começou a ser pesquisada por volta da década de 80, quando passaram a buscar uma união entre a computação e as leis da física e da mecânica quântica em virtude das previsões de limite para a redução na escala da tecnologia usada na computação e para melhor manipulação dos componentes no caso de sucesso com sua redução. Tais previsões foram propostas com base no que ficou conhecido como lei de Moore, a qual, de modo resumido, dizia que o número de transistores nos computadores, e o poder de processamento deles, dobraria a cada 2 anos (Moore, G.E., 1965). E se manteve válida. (Junior, A.C.)

## 3.1 Lei de Moore

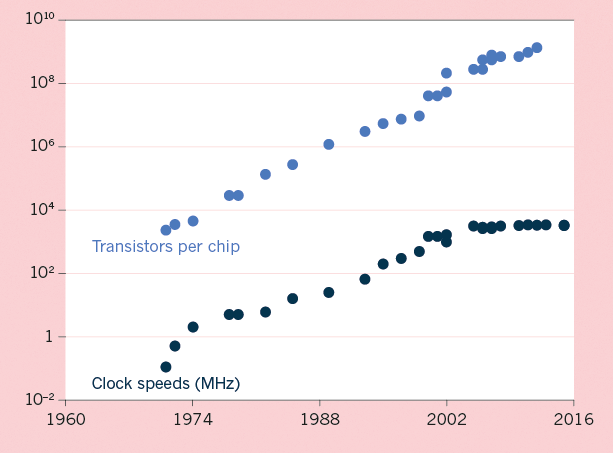
Até 1965, não havia previsões reais sobre o futuro dos hardwares. Isso mudou depois de Gordon Earl Moore (um dos fundadores da Intel) e um conceito estabelecido e publicado pelo mesmo na revista Eletronic Magazine em abril do mesmo ano. Era sua previsão para o mundo da tecnologia, mais especificamente, sobre o poder de processamento dos computadores com base no conhecimento e experiência que adquirira trabalhando na indústria de fabricação de processadores e circuitos para computadores, o que inclui os avanços tecnológicos e conquistas de sua empresa e de outras até aquele momento. Moore disse em seu artigo que o número de transistores, e consequentemente o poder e desempenho das máquinas, ou chips, dobrava a cada ano (Moore, G.E., 1965).

“The complexity for minimum component costs has increased at a rate of roughly a factor of two per year […]. Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years. That means by 1975, the number of components per integrated circuit for minimum cost will be 65,000.”(Moore, G.E., 1965)

“A complexidade para componentes com custos mínimos tem aumentado em uma taxa de aproximadamente um fator de dois por ano [...]. Certamente em um curto prazo pode-se esperar que esta taxa se mantenha, se não aumentar. A longo prazo, a taxa de aumento é um pouco mais incerta, embora não haja razões para se acreditar que ela não se manterá quase constante por pelo menos 10 anos. Isso significa que em torno de 1975, o número de componentes por circuito integrado para um custo mínimo será 65.000”. (Moore, G.E., 1965)

A profecia de Moore foi chamada de ‘Lei’ alguns anos depois e após algumas revisões, redefiniu para em torno de 2 anos o tempo que levaria para o número de transistores nos chips dobrar. Sendo os processadores do computador um dos exemplos mais comuns de chip. O futuro que previra em seu artigo, logo foi se tornando realidade, nas décadas de 1970 e 1980, com o surgimento de produtos usando microprocessadores (Moore, G.E., 1975).

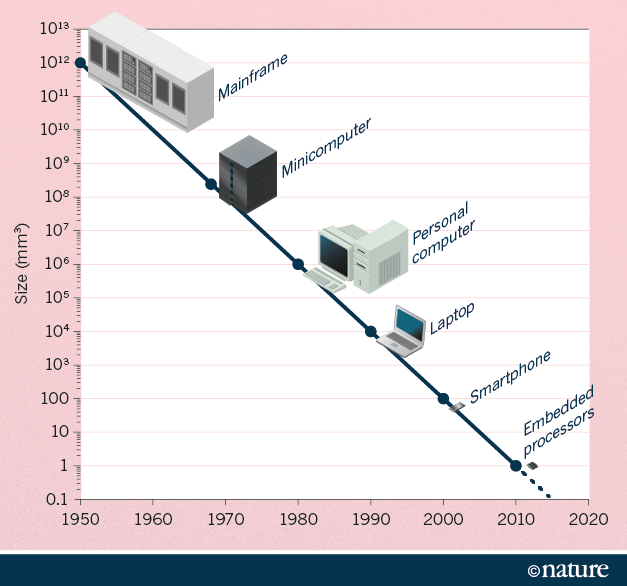
**Figura 3 – Quantidade de transistores em chips e Velocidade de processamento X Tempo**



**Fonte: *Nature* (Fonte: Intel).**

O que era uma ideia, uma previsão para o futuro da tecnologia, causou uma mudança no foco da indústria e passou a ser usado como objetivo de empresas da área, levando-as a investir bastantes recursos buscando resultados que seguissem a Lei de Moore (Khan H. N., et al, 2018). Hardwares melhores e com custos cada vez menores, mais acessíveis, surgiram em virtude dessa busca. Tal desenvolvimento acelerado garantiu que a ideia exposta em 1965 fosse tão importante e perdurasse por tanto tempo no ambiente da pesquisa e desenvolvimento.

**Figura 4 – Evolução das máquinas com as décadas (Tamanho X Tempo).**



**Fonte: *Nature* (Fonte: SIA / SRC).**

Uma forma de continuar aumentando a quantidade de componentes e sua velocidade, foi desenvolvendo-os em escalas cada vez menores. Essa redução no tamanho dos transistores tornava os equipamentos da indústria obsoletos, criando uma necessidade de atualização desses. No entanto, as vantagens que traziam tornavam-nos muito eficientes e atrativos, com isso, o lucro para as empresas compensaria os gastos com a renovação dos equipamentos das fábricas (Brito, A. V.).

“Isso foi caro. Melhorar o desempenho de um microprocessador significava reduzir os elementos de seu circuito de modo que mais deles pudessem ser empacotados juntos no chip, e os elétrons poderiam se mover entre eles mais rapidamente. O escalonamento, por sua vez, exigiu grandes refinamentos na fotolitografia, a tecnologia básica para gravar esses elementos microscópicos em uma superfície de silício. Mas os tempos de boom eram tais que isso pouco importava: um ciclo de auto reforço se instalou. Os chips eram tão versáteis que os fabricantes podiam fabricar apenas alguns tipos - processadores e memória, principalmente - e vendê-los em grandes quantidades. Isso lhes deu dinheiro suficiente para cobrir o custo de modernizar suas instalações de fabricação, ou "fábricas", e ainda reduzir os preços, alimentando ainda mais a demanda. ” (Waldrop, M.M., 2016).

Apesar do grande desenvolvimento, há um limite para a Lei de Moore, que já era previsto que fosse atingido próximo de 2020, e a tecnologia já está perto de alcança-lo. Com transistores na ordem de nanômetros, mesma escala de alguns vírus, esse limite fica mais evidente com aumento de consumo de energia e dissipação de calor. É um grande número de transistores operando em conjunto através da passagem de corrente, com uma boa parte dela sendo dissipada. E alguns limites ainda mais fundamentais devem surgir em menos de uma década (Waldrop, M.M., 2016; Khan H. N., et al, 2018; Junior, A.C.).

Em 2015, já era visto que as velocidades dos chips já não aumentavam como antes havia um tempo, os custos de transistores individuais haviam estabilizado e o tempo entre as novas gerações havia se estendido. A aceleração prevista pela Lei de Moore havia caído (Markoff, J., 2015).

Uma saída encontrada uma vez que o fim da Lei de Moore ficava mais próximo, foi a computação quântica, onde as leis da física passam a ser mais complexas. Saem do campo da física clássica para abordar a área quântica. Nessa união da mecânica quântica com a computação, a unidade básica de informação passa de *bit* para *qubit*, o qual além de assumir os valores 0 ou 1, possui o diferencial de poder assumir os dois valores ao mesmo tempo (Rieffel, 2000). Essa propriedade particular que expande o poder computacional de um computador quântico, com o potencial para o processamento paralelo. A experiência conhecida como “divisão de raio”, ilustra o fenômeno quântico.

## 3.2 Experiência com fótons

O experimento usa uma fonte de luz direcionada a uma lente e dois sensores ópticos (A e B), colocados de forma que detectem as duas possíveis trajetórias que o raio pode ter ao passar pela lente. A fonte manda apenas um fóton por vez e repete esse procedimento diversas vezes. Como o fóton é indivisível, espera-se que seja refletido aleatoriamente para um dos sensores e é o que ocorre. Em metade dos casos ele é detectado por A e na outra metade, por B. Nesse ponto, tanto a física clássica concorda com a quântica.

A diferença na forma como a física quântica interpreta os fatos, de forma menos intuitiva. Ela afirma que o fóton passa pelas duas trajetórias simultaneamente em todos os casos. Tal afirmação é verificada ao realizar uma nova experiência, onde são adicionados dois espelhos e mais uma lente, a qual é idêntica à primeira e os espelhos sempre refletem a luz na mesma direção.

Novamente emite-se 1 fóton por vez, diversas vezes. Diferentemente do anterior, nesse experimento apenas um dos sensores detecta o fóton, o mesmo em todas as vezes. Assim, a probabilidade de um dos sensores (A ou B) ser atingido é de 100% e a do outro é nula. A explicação para tal é que o fóton percorre os dois caminhos possíveis ao mesmo tempo e cria uma interferência no ponto de intersecção, na segunda lente, que anula a probabilidade de o outro sensor receber o fóton. Chama-se esse efeito de *single-particle interference*. Ou seja, todas as possibilidades de fato ocorrem, mas quando observado, o sistema entra em colapso, resultando em apenas uma ocorrência em particular, conhecida como realidade (como observado na primeira experiência). Portanto o fato de observar um sistema já influencia seu desfecho.

Para observar que as duas trajetórias são percorridas simultaneamente, é preciso colocar um obstáculo em uma das trajetórias, pois assim o outro caminho fica livre até o fim e os sensores voltam a registrar o fóton como na primeira experiência, ou seja, com 50% de probabilidade.

## 

## 3.3 Primeiros avanços

Paul Benioff em 1981, foi o primeiro a aplicar teorias quânticas para computadores com sua Máquina de Turing quântica. A Máquina de Turing consiste em uma fita dividida em células, que se move para a direita ou para a esquerda, lendo e gravando informações em *bits*. Já a máquina quântica de Benioff, continha células que podiam comportar o estado de superposição do *bit* quântico. O problema para construir um computador quântico estava na manipulação dos *qubit* sem alterar a informação que carregam, pois até uma alteração qualquer pode alterar o seu estado.

Em 1981, em uma conferência no MIT, o físico Richard Feynman afirmou que a computação clássica não seria capaz de modelar com eficiência sistemas da mecânica quântica, os quais só poderiam ser modelados por outro sistema quântico. Como solução, propôs a utilização de sistemas quânticos em computadores, que desenvolveriam um processamento superior aos computadores comuns e seriam muito uteis nessas simulações de experimentos da física quântica. Tais máquinas ainda não existiam, mas poderiam ser criadas e poderiam também servir como um simulador quântico universal (Feynman, R.P., 1981; Melo, B.L.M; Christofoletti, T.V.D., 2003; Junior, A.C.).

Em 1985, David Deustsch, da Universidade de Oxford, fez a descrição do primeiro computador quântico universal, que seria capaz de simular o funcionamento de outro computador quântico e cria também o primeiro algoritmo quântico.

## 3.4 Manipulação de dados e erros quânticos

Somente em 1994, no Bell Labs da AT&T em Nova Jersey, houve mais uma descoberta de grande destaque na área. Peter Shor, professor de matemática aplicada, desenvolveu um excelente algoritmo e o publicou no artigo “*Algorithms for Quantum Computing: Discrete Logarithms Factoring*”. Ficou conhecido como Algoritmo de Shor. Ele podia, através de propriedades do computador quântico, fatorar grandes números (na ordem de dígitos) a uma velocidade inovadora. Foi o primeiro algoritmo a usar funcionalidades únicas de um computador quântico para otimizar a solução de um problema.

Através da superposição quântica e funções quânticas especificas, ele reduzia a complexidade do tempo de fatoração de exponencial para polinomial. E uma aplicação imediata para o algoritmo de Shor é na criptografia, onde a segurança dos sistemas de chave pública baseiam-se na dificuldade de fatoração de números muito grandes. Um computador que possa realizar os cálculos de forma rápida comprometeria a segurança desses sistemas.

Dois anos depois, Lov Grover, também no Bell Labs, desenvolveu o Speedup, o primeiro algoritmo para uma pesquisa de base de dados quânticos. No mesmo ano, foi proposto pela comunidade cientifica o primeiro modelo para correção de erro quântico.

## 3.5 Primeiras maquinas

Em 1999, construíram os primeiros protótipos de computadores quânticos com base em montagem térmica, feitos no MIT.

### 2.5.1. IBM

Em dezembro de 2001, foi construído um computador quântico de 7 *qubits* pelos cientistas do Centro de Pesquisas da IBM (*International Business Machines Corporation*) em Almaden. Com o algoritmo de Shor implementado, ele conseguiu fatorar corretamente o número 15. Era um resultado simples, mas ele mostrou que a computação quântica era viável, embora ele ainda não fosse o suficiente para quebrar um sistema de criptografia. As maiores dificuldades eram tecnológicas e não teóricas. Um exemplo era a alta incidência de erros nos computadores quânticos.

O computador foi implementado através de uma molécula com 7 spins, sendo seu núcleo constituído por 5 átomos de flúor e 2 de carbono. A programação era feita por pulsos de radiofrequência e a leitura de resultados, por ressonância magnética nuclear (RMN), similar à tecnologia de aparelhos de tomografia computadorizada de hospitais. Para ser operado, exigia baixas temperaturas para reduzir os erros.

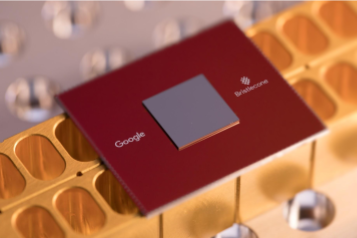
### 2.5.2. Computador híbrido

Em 2004, uma equipe liderada por Charles Bennett, realizou pela primeira vez o teletransporte com átomos, isso é, comunicação de informações de 2 pontos distantes sem que a informação percorresse essa distância. Anos depois, em 2007, foi criado um computador híbrido com processador quântico de 16 qubits que realizaria tarefas praticas, como resolver problemas lógicos e soluções para jogos de Sudoku. Nascia o Orion, desenvolvido pela canadense D-Wave. No mesmo período, a Universidade de Yale, nos Estados Unidos, criou seu primeiro computador quântico rudimentar que também executava operações simples.

Em 2011, a D-Wave lançou o primeiro computador quântico para comercialização, o D-Wave One, com um processador de 128 qubits. No entanto, ainda precisava ser utilizado em conjunto com computadores convencionais.

E desde então, a pesquisa não parou, levando a novos modelos, tecnologias e descobertas na área. Empresas inclusive formam parcerias buscando avanços. Como a Google e Nasa que juntas conseguiram um computador quântico com o processador Bristlecone que possui 72 qubits (Kelly, 2018).

**Figura 5 – Bristlecone, o novo processador quântico da Google.**



**Fonte: Google Al Blog.**

# 4 CONCEITOS DA MECÂNICA NA COMPUTAÇÃO QUÂNTICA

Dentro do escopo analisado, a computação quântica cerca termos e comportamentos que prescrevem, de alguma forma, os *qubits* de forma geral, com isso efeitos que os descrevem são importantes para a aplicação, alguns exemplos destes são a codificação densa e o teletransporte.

## 4.1 Codificação densa

A codificação densa (**Charles H. Bennett**) é baseada no efeito de partículas denominado *estado de Bell* ([**John S. Bell**](https://en.wikipedia.org/wiki/John_S._Bell))*.* Esse, por sua vez é dado para um efeito que descreve a relação entre duas partículas de tal maneira em que ao separa-las, independentemente de sua distância, ao realizar o efeito em uma, imediatamente, a outra replica o mesmo efeito.

Ao gerar um par de partículas que satisfazem |ψ+〉 (funções de ondas iguais) na qual podem ser geradas pelo produto do decaimento de um átomo, ações realizadas em uma partícula replicarão em outra modificado seu estado emaranhado através de operadores unitários. Então, para transportar informação através de *qubits* de um ponto A para o B, antes da ação requisitada, é necessário obter duas partículas em tal estado e enviar uma para B partindo de A. Essas unidades serão armazenadas até a unidade em A ser alterada, e por consequência, alterando em B que será transformada em informação em um instante de tempo.

## 4.2 Teorema no-cloning

O teorema chamado de *no-cloning* (**Wootters et al, 1982**), afirma que não é possível criar cópias idênticas de um estado quântico arbitrário desconhecido, ou seja, não há uma máquina para se copiar estados quânticos. Suponha |0〉*A e* |1〉*A* sendo um estado arbitrário |**x**〉*A* na qual o objetivo seja copia-lo, ou seja, uma máquina com tal capacidade entraria com dois estados diferentes e sua saída resulta em dois estados iguais. Para o sentido de clonagem dado, literalmente todos os estados, partículas, interações e níveis energéticos devem ser os mesmos para ambos os corpos. A partir da preliminar de distribuição das transformações na sobreposição de estados, ao clona-los de modo separados, . Porém quando copiado uma partícula com sobreposição de estados tal distribuição não é respeitada, pois a transformação (clonagem) separada resulta no produto de seu próprio estado e . Portanto não pode haver coexistência da clonagem na mecânica quântica

# 5 ALGORITMOS PARA COMPUTADORES QUÂNTICOS

Escrever algoritmos para tais computadores exigem uma abordagem diferente para sua construção, já que a arquitetura representa a execução de vários estados ao mesmo tempo. Portanto, para utiliza-los haverá uma entrada (input) clássica e assim, processa-lo em um estado quântico definido por uma superposição em escala exponencial de estados clássicos, na qual engloba transformar estados que codificam o problema, para o estado codificado da solução. Um exemplo de algoritmo com essa proposição é o denominado algoritmo Shor’s ([**Shor**](https://en.wikipedia.org/wiki/Peter_Shor)**, 1994**) em que determina o fatorial de um número milhões de vezes mais rápido do que a forma clássica, descrita por um fator de complexidade O(e1.9 (log N)1/3 (log log N)2/3). Porém o número máximo possível a se fatorar com essa tecnologia foi 15.

Ao viabilizar o poder de processamento na escala de um computador quântico, pode-se supor um algoritmo, por exemplo, que busca itens em uma lista (**Morello apud Grover, 1996**). Esse algoritmo propõe o uso do paralelismo quântico para diminuir a quantidade de passos em uma ordem de , onde representa o número total de itens em uma lista. Para exemplificação, será usado uma lista de 8 números telefônicos associados a nomes. Como os números de telefone não estão em ordem, para um algoritmo clássico encontrar pelo referido atributo seria necessário passar pelos 8 registros a fim de comparar o valor desejado com cada valor, para um algoritmo quântico será usado 3 qubits para codificar cada unidade de informação desejada, no caso número de telefone, portanto seus estados estarão para |001〉, |110〉, |100〉, |010〉, |011〉, |000〉, |101〉.

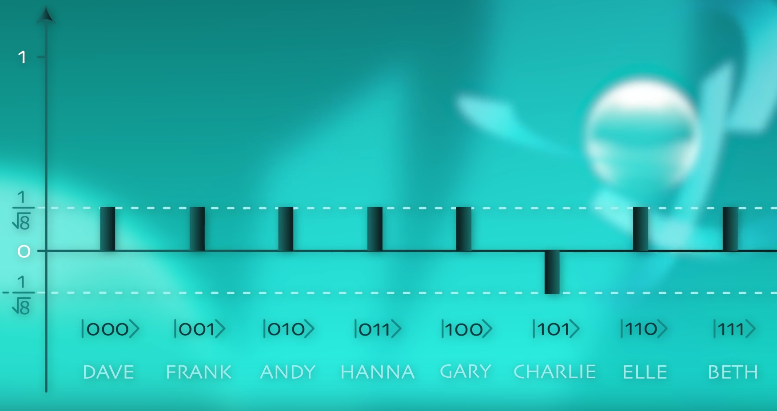
**Tabela 1 – números codificados na lista de nomes**

|  |  |
| --- | --- |
| Nome | Estado |
| Dave | |000〉 |
| Frank | |001〉 |
| Andy | |010〉 |
| Hanna | |011〉 |
| Gary | |100〉 |
| Charlie | |101〉 |
| Elle | |110〉 |
| Beth | |111〉 |

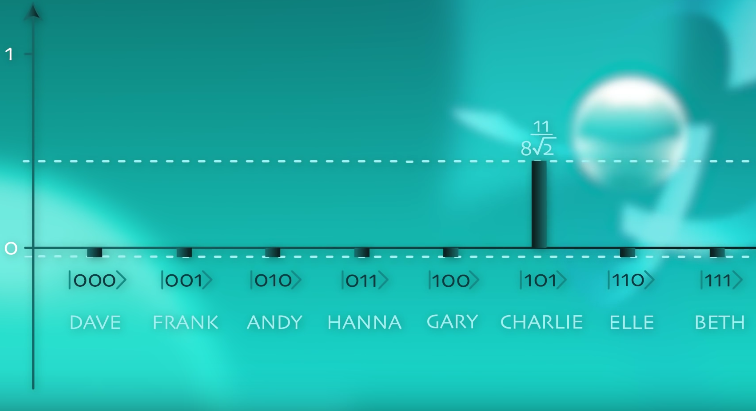
**Fonte: Australia’s Global University**

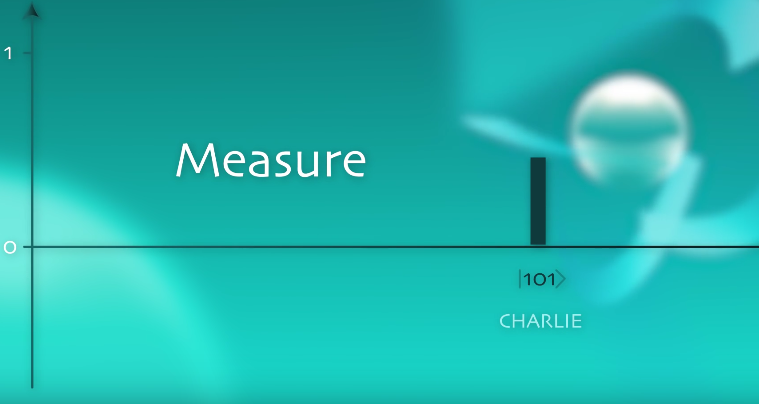
Suponha que o objetivo seja encontrar o registro associado ao estado |101〉, primeiramente, deve ser criado uma superposição de todos os estados possíveis para a quantidade de qubits inseridas. Na mecânica quântica é dotado que cada parte da amplitude da superposição indica como ela é incluída dentro desse escopo, e a raiz quadrada da amplitude de cada parte indica um código em particular. No exemplo, dotando cada parte como uma variável de “a” até “h” teremos a probabilidade de medir cada um de todos os códigos . A partir deste ponto é rodado um script globalmente para todos os estados que altera sua amplitude, aumentando a probabilidade de ser encontrado a cada passo rodado, obedecendo a ordem . A seguir imagens gráficas representativas de cada rodada do algoritmo e sua respectiva amplitude de probabilidade.

**Figura 6 – Rodada 0 em algoritmo de busca paralela****Fonte: Australia’s Global University**

**Figura 7 – Rodada 1 em algoritmo de busca paralela** **Fonte: Australia’s Global University**

**Figura 8 – Rodada 2 em algoritmo de busca paralela****Fonte: Australia’s Global University**

**Figura 9 – Rodada 3 em algoritmo de busca paralela** **Fonte: Australia’s Global University**

**Fotografia 10 – Rodada final em algoritmo de busca paralelaFonte: Australia’s Global University**

**5.1 Criptografia e possíveis conflitos**

Sem dúvidas, a capacidade de informação processada por paralelismo é a maior vantagem de um computador quântico, porém, ao passo que se apresenta como uma reestruturação no modo que as máquinas funcionam, conflitos sobre as duas variáveis se tornam evidentes.

Um algoritmo como de Lov Grover que aparenta ser apenas uma simples tentativa de se processar um algoritmo quântico para futuras aplicações, por exemplo, pode parecer inocente, até o dado instante na tentativa de busca para uma senha correta dentre uma lista de todas possíveis, computadores quânticos possuem tal processamento para testar todos os casos de criptografias com chaves públicas rapidamente. O poder e segurança da maior parte de métodos criptográficos tradicionais podem estar sendo ameaçados (**Bernstein, Lange, 2017**), alguns como o sha-256, AES-128, AES-156 e Salsa20 ainda podem ser levados em consideração contra quebras dessa nova arquitetura, por possuírem um tamanho de tokenização alto. Para uma possível solução, há uma área de estudo denominada de encriptação pós-quântica. Para uma possível solução deste problema, a criptografia pós quântica se baseia em conceitos da mecânica quântica para combater capacidades quânticas. Basicamente a atual criptografia utiliza sistema de chaves de encriptação e decriptação para assegurar a não violação de dados (**Vahed apud Diffiem, 1977**), duas chaves são construídas para esse sistema, um que apenas pode codificar a mensagem e outro que apenas pode decodificar. A chave codificadora pode ser enviada livremente na relação de servidor-cliente, pois um interceptador da mensagem terá a chave de codificação e a mensagem criptografada, portanto não poderá visualiza-la. Apenas os servidores possuem a chave de decodificação e por isso, podem manter a segurança desses dados. Resumidamente, um usuário que queira enviar uma mensagem para o servidor utiliza a chave de codificação para faze-la, e envia essa mensagem. O interceptador irá criar uma cópia dessas informações, porém nada poderá fazê-lo já que não pode decodifica-la, o servidor por outro lado possui a chave para retornar os dados em seu estado normal, concluindo de forma segura a tarefa de transporta-la.

Essa segurança só existe por conta da dificuldade na confecção de uma chave decodificadora, pois a partir de uma codificadora é possível criar a sua chave, porém seu custo computacional é inimaginável, tornando esse processo inviável. Para um computador quântico isso não seria um problema, sua capacidade permitiria essa quebra e a partir deste ponto a criptografia pós quânticas entra em processo. Ao gerar uma informação clássica com bits, é possível gerar *qubits* com suas orientações na qual permitam ao serem descobertos seu direcionamento a partir de uma sobreposição.

# 6 COMPUTAÇÃO QUÂNTICA E SOCIEDADE: COMO TORNAR REAL A COMPUTAÇÃO QUÂNTICA?

Ao se discutir como tornar a computação quântica algo real é imprescindível primeiro estabelecer um conceito muito importante sobre o que é um computador quântico, para isso o físico David P. DiVincenzo, estabeleceu cinco problemas ou requisitos que devem ser implementados ou solucionados afim de se criar um computador quântico. (**DiVincenzo,1996,2000; Gouvêa**)

**Figura 11 - David P. DiVincenzo**



**Fonte – RWTH Aachen University**

## 6.1 A forma do qubit

O primeiro requisito é de um sistema físico escalável com qubits bem definidos, é necessário que exista uma entidade com a capacidade de representar o qubit, que obedeça aos critérios de comportamento quântico e que possa suportar os diversos estados do qubit (0, 1 ou 0 e 1). Além disso deve-se conhecer o mecanismo para se manipular os qubits, assim como suas características internas. (**DiVincenzo,1996,2000; Gouvêa**)

Uma boa caracterização do qubit, significa dentre muitas coisas que seus parâmetros físicos devem ser precisamente conhecidos, entre tais parâmetros podemos citar o espaço de Hilbert, a hamiltoniana interna do qubit, a presença de acoplamentos com outros estados de qubit, interação com outros qubits e acoplamentos com campos externos. Tais conhecimentos são de extrema importância para a realização da correção de erro quântica que será abordada mais à frente. (**DiVincenzo,2000**)

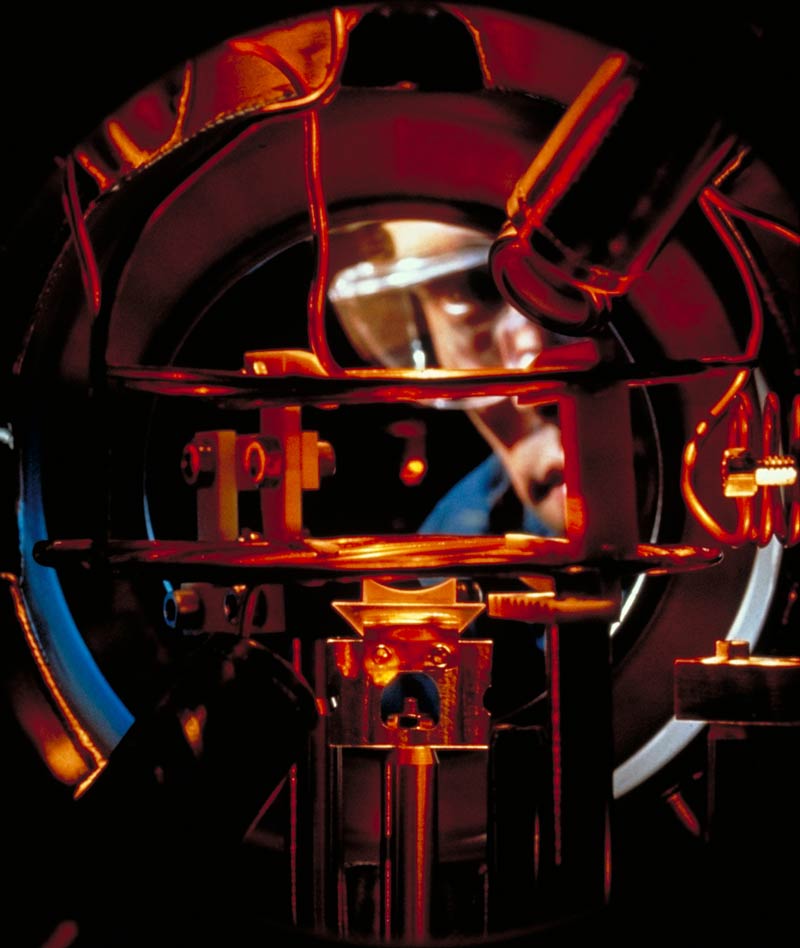
## 6.2 O estado inicial do qubit

O segundo diz respeito a habilidade de definir o estado inicial dos qubits, a exemplo │000...›, apesar desse requisito ser aparentemente simples e até lógico, ao considerar que para se realizar uma computação deve-se conhecer o estado inicial do sistema. Uma segunda razão para isso é para se realizar aplicações na correção de erro quântico, a qual requer um fornecimento constante de qubits com um baixo estado de entropia (│0›), outra importante aplicação disso é que o tempo para se zerar um qubit é de extremo impacto na velocidade total da aplicação. **(DiVincenzo,1996,2000; Gouvêa**)

Se tal tempo utilizado para realizar essa inicialização for extremamente longo, se comparado com o tempo de operação das portas logicas o Físico DiVincenzo, ressalta que seria necessária utilizar uma técnica na qual os qubits seriam inicializados fora da região onde se está realizando a computação e após isso seriam inseridos novamente no Sistema, a qual ele denomina *“conveyor belt”.* (**DiVincenzo ,2000**)

Afim de se zerar o qubit, ou seja deixar ele em um estado de baixa entropia, é necessário chegar até seu estado hamiltoniano de interesse, para tal o sistema pode ser tanto naturalmente resfriado, ou o processo pode ser realizado através de uma medida que projete o sistema, ou outro que possa ser transformado no mesmo; um dos possíveis meios de se resfriar naturalmente um qubit é através de resfriamento a lazer, que é um dos mais usados para se resfriar partículas aprisionadas, ou através da ressonância de spins dos elétrons, entretanto esses métodos de resfriamento possuem uma problema muito importante , pois independentemente do método escolhido o tempo de resfriamento não será menor que o tempo de decorrência, o que causaria uma necessidade de usar a técnica mencionada anteriormente para resolver tal problema.( **DiVincenzo,2000**)

**Figura 12 – Cientista Observando Átomo sobre aprisionamento.**



**Fonte - Physics central**

**Figura 13 – Laboratório de resfriamento a lazer e aprisionamento NIST (Gaithersburg, MD).**



**Fonte - Physics central**

## 6.3 Tempo de Decorrência

O terceiro tópico citado é relacionado com os tempos de decorrência, aonde estes devem mais longos que o tempo de operação das portas. Uma característica importante de um sistema quântico e consequentemente de um qubit é que, com o tempo, ele interage com o ambiente e seu estado é alterado imprevisivelmente. Esse tempo é chamado tempo de decorrência, e consiste em um dos principais problemas da computação quântica, tal estado possui muitas implicações na computação quântica, muitas das quais tendem a inviabilizar a mesma, uma destas implicações é o erro quântico. (**DiVincenzo,1996,2000; Gouvêa**)

Tal problema era de tanta importância para a computação que acreditavam que ele definitivamente era um fator que impedia a computação quântica, entretanto, Peter W. Shor provou que era possível contornar este problema utilizando códigos para a correção de erro quânticos. (**Gouvêa**, **Calderbank e Shor,1996**)

Sem entrar em muito detalhamento a correção de erro quântico é similar à correção de erro comum na qual são usados alguns bits para detectar e corrigir os erros, entretanto a correção de erro quântica é muito mais complicada do que só isso, pois ao invés de lidarmos com dados binários temos que lidar com estados quânticos no processo. (**Rieffel e Polak, 2000**)

A correção de erro quântica precisa reconstruir o estado do qubit, entretanto dado a impossibilidade de clonar ou de copiar o estado quântico, essa reconstrução é mais difícil que no caso clássico, o que implica que as técnicas clássicas, apesar de servirem de base para os códigos quânticos não podem ser simplesmente modificadas para trabalhar com sistemas quânticos. (**Rieffel e Polak, 2000; Calderbank e Shor,1996**)

Ainda segundo Shor para se realizar a correção de erro quântico, é preciso medir a decorrência sem perturbar a informação previamente codificada, ou em outras palavras medir a decorrência sem observar o estado codificado, isso permite corrigir a decorrência enquanto o estado mapeado fica imutado. (**Calderbank e Shor,1996; Shor,1995**)

**Figura 14 – Peter W. Shor**



**Fonte - MIT**

## 6.4 Portas Lógicas

O quarto ponto citado elo DiVincenzo, é um conjunto universal de portas quânticas, assim como a computação clássica possui portas logicas, a computação quântica necessita de portas logicas equivalentes, para se realizar computação sobre os qubits. É importante notar que portas quânticas não podem ser implementadas perfeitamente; elas também podem causar erros. Contudo, tais erros podem ser contornados com o mesmo mecanismo de correção de erro usado para a decorrência. (**DiVincenzo,1996,2000; Gouvêa**)

## 6.5 Leitura do Qubit

O último requisito citado, apesar de ter ficado por último é um dos mais importantes este seria a capacidade de se medir qubits específicos, que é um requisito natural: evidentemente é necessário poder ler o resultado de uma computação de modo confiável. Este fator também é importante na correção de erro quântico. (**DiVincenzo,1996,2000; Gouvêa**)

## 6.6 Computação Quântica no Brasil

Atualmente o Brasil apesar de estar muito atrás das grandes potencias como a União europeia, China, Estados Unidos e Canadá, já conta com certos investimentos na área da computação quântica, no brasil podemos destacar dois grupos de pesquisas em relação a essa área o LNCC (Laboratório Nacional de Computação Científica) e o INCT-IQ (Instituto Nacional de Ciência e Tecnologia de Informação Quântica)

Sobre o Laboratório Nacional de Computação Cientifica, o seu grupo voltado a computação quântica está no LNCC um instituto do Ministério de Ciência, Tecnologia e Inovação (MCTI) na Cidade Imperial de Petrópolis, no estado do Rio de Janeiro, e tem como missão desenvolver pesquisa original nas áreas de computação quântica e informação quântica, além de supervisionar estudantes de mestrado e doutoramento na área. O grupo possui diversos trabalhos e publicações relacionadas a algoritmos quânticos e a Caminhos Quânticos (*Quantum Walks.).* (**Lara, 2015; Oliveira 2007**)

Enquanto isso, o Instituto Nacional de Ciência e Tecnologia de Informação Quântica tem como o objetivo o desenvolvimento de pesquisas básicas que conduzam ao desenvolvimento de tecnologias de computação e comunicação quântica, o instituto possui diversas parcerias com muitas faculdades do país. São 20 grupos de pesquisa, 12 laboratórios, em 15 instituições localizados em sete estados do país, que formam a rede científica do instituto. A maioria dos diversos grupos do INCT-IQ, possuem diversos trabalhos em suas respectivas áreas de pesquisas que variam de Codificação Quântica a Teoria de Informação Quântica.

|  |  |  |
| --- | --- | --- |
| Grupo | Sigla | Instituição |
| Enlight | ENLIGHT | UFMG |
| Grupo de Caos Quântico e Informação Quântica | GCQIQ | CBPF |
| Grupo de Informação e Computação Quântica | GICQ3 | UFU |
| Grupo de Informação Quântica | GIQ | UFABC |
| Grupo de Informação Quântica | GIQ2 | UEPG |
| Grupo de Informação Quântica e Fenômenos Críticos | GIQFC | UFF |
| Grupo de Informação Quântica Teórica | GIQT | UFSCar/USP-São Carlos |
| Grupo de Matéria Condensada Teórica | GMCT | UFRJ |
| Grupo de Óptica Quântica e Informação Quântica | GOIQ | UFRJ |
| Grupo de Óptica e Informação Quântica | GOIQ2 | UFF/UFF-Volta Redonda |
| Grupo de Óptica e Materiais | GOM | UFAL |
| Grupo de Óptica Quântica | GOQ | UNICAMP |
| Grupo Processamento da Informação Quântica por Ressonância Magnética Nuclear | GPIQRMN | CBPF; USP/São Carlos; UFES |
| Grupo Teoria da Codificação Quântica | GTCQ | UNICAMP |
| Laboratório de Colisões Atômicas e Moleculares | LACAM | UFRJ |
| Laboratório de átomos Frios | LAF | UFRJ |
| Laboratório de Tecnologia da Informação Quântica | LATIQ | UFC |
| Laboratório de Comunicações Quânticas | LCQ | PUC-RIO |
| Laboratório de Interações Atômicas | LIA | USP/São Carlos |
| Laboratório de Informação Quântica com Sistemas Atômicos | LIQA | UFPE |
| Laboratório de Manipulação Coerente de Átomos e Luz | LMCAL | USP |
| Laboratório de Óptica Quântica | LOQ | UFRJ |
| Grupo de Teoria | T1 | UNICAMP |
| Grupo de Teoria | T2 | USP |

**Tabela 2 – Grupos do INCT-IQ**

**Fonte – INCT-IQ**

**CONCLUSÃO**

A computação quântica surgiu da necessidade de melhores maquinas, uma vez que a computação clássica, ou comum, não daria conta de simular certos sistemas, que envolviam simulações quânticas ou possuíam alta complexidade, exigindo um processamento de soluções mais veloz. Como com a maioria das invenções, seu início foi bastante teórico e permaneceu assim por anos, devido aos desafios de criar algo novo e principalmente por causa da relação com a mecânica quântica, um ambiente cheio de incertezas e que a menor interferência externa pode alterar todo um experimento.

Muitos nomes fizeram parte de seu desenvolvimento, como Feynman, físico responsável pela proposta da computação quântica como solução para o momento em que os computadores comuns já não servissem; Shor com seu algoritmo inovador e empresas como a D-Wave, que buscou a criação de um computador quântico cada vez melhor e surpreende a cada lançamento.

Por ainda se tratar de máquinas grandes, que requerem uma temperatura muito baixa para sua operação correta e com menor índice de erros, é uma tecnologia que na maioria dos casos, senão sempre, está associada às grandes empresas do ramo da computação, que são as que podem investir na área e terão benefícios claros, e aplicações imediatas até, em caso de sucesso. Como exemplo pode-se citar a Google, a D-Wave e a IBM.

A tecnologia e o conhecimento da área quântica cresceram e melhoraram ao longo do tempo em que ela vem sendo pesquisada e com isso novas oportunidades surgiram, mas sua complexidade e sensibilidade ao erro continuam dificultando o avanço dessa tecnologia. Mesmo em meio a esses desafios, parcerias visando o desenvolvimento de novas máquinas surgem, fazendo com que a computação quântica não fique estagnada e se aproxime cada vez mais daquilo que foi proposto (máquinas que superariam e muito o poder de processamento dos computadores comuns de modo que possuísse funções além da capacidade desses).

Ainda levará um tempo até que seja possível manipular o qubit livre e precisamente, sem o grande índice de erros, com um melhor controle desses. Mas o a computação quântica está mais próxima do que se imagina, é necessário apenas mais desenvolvimento, tecnológico e teórico, para um melhor aproveitamento dela e o Brasil está envolvido com pesquisas originais sobre informação e computação quântica, além de pesquisas para desenvolvimento de novas tecnologias de computação e comunicação quântica.

**REFERÊNCIAS**

Berg, Bernd A. **A Short History of Physics**. Disponível em: <http://www.hep.fsu.edu/~berg/teach/phy1090/HistoryPhys.pdf>. Acesso em: 10 set. 2018.

Brito, A. V., **Introdução a Arquitetura de Computadores**

Disponível em: < http://producao.virtual.ufpb.br/books/edusantana/introducao-a-arquitetura-de-computadores-livro/livro/livro.pdf >. Acesso em: 10 set. 2018.

Calderbank, A. R. e Shor, Peter W. **Good quantum error-correcting codes exist.** Disponível em: < https://arxiv.org/pdf/quant-ph/9512032.pdf>. Acesso em: 13 set. 2018.

Chibeni. Silvio S. **Certezas e incertezas sobre as relações de Heisenberg**. Disponível em: <http://www.unicamp.br/~chibeni/public/heisenberg.pdf>. Acesso em: 11 set. 2018 .

DiVincenzo, David P. **The Physical Implementation of Quantum Computation.** Disponível em: < https://arxiv.org/pdf/quant-ph/0002077v3.pdf>. Acesso em: 13 set. 2018.

DiVincenzo, David P. **Topics in quantum computers.** Disponível em: < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.242.2165&rep=rep1&type=pdf>. Acesso em: 13 set. 2018.

D-Wave Systems Inc. [CA]. **The D-Wave 2000Q Quantum Computer – Technology Overview.** Disponível em: < https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral\_0718web.pdf >. Acesso em: 13 set. 2018.

Farias, Robson F. **A Dualidade Onda-Partícula**. Disponível em: <https://www.researchgate.net/publication/318445877/download>. Acesso em: 11 set. 2018.

Feynman, R.P., **Simulating Physics with Computers.** 1981

Disponível em: < https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf >. Acesso em: 12 set. 2018.

Gouvêa, Conrado P. L. **Introdução à Computação Quântica.** Disponível em: < http://www.ic.unicamp.br/~ducatte/mo401/1s2008/T2/079724-t2.pdf>. Acesso em: 13 set. 2018.

Greca. Ileana M. **Superposição linear em ensino de mecânica quântica**. Disponível em: <http://www.cienciamao.usp.br/dados/rab/\_superposicaolinearemensi.artigocompleto.pdf>. Acesso em: 12 set. 2018.

Grover, Lov K. **A fast quantum mechanical algorithm for database search**. Disponível em: <<https://dl.acm.org/citation.cfm?id=237866>>. Acesso em: 9 set. 2018.

Junior, A.C., **COMPUTAÇÃO QUÂNTICA.**

Disponível em: < <http://periodicos.unesc.net/sulcomp/article/viewFile/2068/1958>>. Acesso em: 8 set. 2018.

Khan, H.N., et al. **Science and research policy at the end of Moore’s law.**

Disponível em: < https://www.nature.com/articles/s41928-017-0005-9 >. Acesso em: 9 set. 2018.

Kelly, Julian. [**A Preview of Bristlecone, Google’s New Quantum Processor**](http://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html)**.** 2018 Disponível em: < https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>. Acesso em: 13 set. 2018**.**

King, A. D., et al. **Observation of topological phenomena in a programmable lattice of 1,800 qubits.** 2018.

Disponível em: < https://www.nature.com/articles/s41586-018-0410-x >. Acesso em: 12 set. 2018.

Lara, Pedro.C.S. **Global Optimization Algorithms based on Quantum Algorithms**. Disponível em: <http://qubit.lncc.br/files/pcslara\_phd.pdf> Acesso em: 13 set. 2018.

Markoff, J., **Smaller, Faster, Cheaper, Over: The Future of Computer Chips.** 2015

Disponível em: < https://www.nytimes.com/2015/09/27/technology/smaller-faster-cheaper-over-the-future-of-computer-chips.html?\_r=0 >. Acesso em: 12 set. 2018.

Melo, B.L.M; Christofoletti, T.V.D., **Computação Quântica: Estado da Arte**. 2003

Disponível em: http://www.inf.ufsc.br/~j.barreto/trabaluno/TCBrunoTulio.pdf >. Acesso em: 8 set. 2018.

Moore, G. E., **Cramming more components onto integrated circuits.** 1965 Disponível em: < https://web.archive.org/web/20090126170054/http://download.intel.com:80/museum/Moores\_Law/Articles-Press\_Releases/Gordon\_Moore\_1965\_Article.pdf >. Acesso em: 11 set. 2018.

Moore, G. E., **Progress In Digital Integrated Electronics.** IEDM Tech. Digest 11–13 (1975). Disponível em: < https://www.eng.auburn.edu/~agrawvd/COURSE/E7770\_Spr07/READ/Gordon\_Moore\_1975\_Speech.pdf >. Acesso em: 11 set. 2018.

Morello, Andrea. UNSW. **Quantum Computing Concepts – Quantum Algorithms**. Disponível em: <https://www.youtube.com/watch?v=8anVNc0r\_8o&t=135s>. Acesso em: 08 set. 2018.

Oliveira, Amanda C. **Simulation of Quantum Walks in Two-Dimensional Lattices.** Disponível em: < http://qubit.lncc.br/files/acoliveira\_phd.pdf> Acesso em: 13 set. 2018.

Rieffel, Eleanor G. e Polak, Wolfgang. **An Introduction to Quantum Computing for Non-Physicists.** Disponível em: < https://arxiv.org/abs/quant-ph/9809016>. Acesso em: 13 set. 2018.

Rigolin. Gustavo. **Emaranhamento quântico**. Disponível em: <https://physicae.ifi.unicamp.br/index.php/physicae/article/view/physicae.7.1/47>. Acesso em: 12 set. 2018.

Santos. Gislan S. **Espaços de Hilbert**. Disponível em: <http://www.ebah.com.br/content/ABAAAAXhcAJ/espacos-hilbert>. Acesso em: 12 set. 2018.

Shor, Peter W. **Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer**. Disponível em: <https://epubs.siam.org/doi/abs/10.1137/S0036144598347011>. Acesso em: 9 set. 2018.

Shor, Peter W. **Scheme for reducing decoherence in quantum computer memory.** Disponível em: <http://www.cs.miami.edu/home/burt/learning/Csc670.052/pR2493\_1.pdf>. Acesso em: 13 set. 2018.

Silva, Edson A. **O efeito fotoelétrico**. Disponível em: <https://pantheon.ufrj.br/bitstream/11422/3097/4/EAPSilva.pdf>. Acesso em: 10 set. 2018.

Vahed, Ahmed. **An overview of modern cryptography**. Disponível em: <https://pdfs.semanticscholar.org/46d6/fee601a4f89b448deff8af7fce9c52d68501.pdf>. Acesso em: 12 set. 2018.

Waldrop, M.M., **The chips are down for Moore’s law.** 2016

Disponível em: < https://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338>. Acesso em: 9 set. 2018.

Wooters, William B. **No-cloning theorem**. Disponível em: <https://www.revolvy.com/page/No%252Dcloning-theorem>. Acesso em: 12 set. 2018