Pró-Reitoria Acadêmica
Escola de Exatas, Arquitetura e Meio Ambiente
Curso de Física
Trabalho de Conclusão de Curso

COMPUTAÇÃO QUÂNTICA: A POSSIBILIDADE DE UM NOVO MUNDO

Autor: Gabriel Carvalho Veloso Dantas
Orientador: Prof. Dr. Paulo Henrique Alves Guimarães

Brasília - DF
2018

GABRIEL CARVALHO VELOSO DANTAS

COMPUTAÇÃO QUÂNTICA: A POSSIBILIDADE DE UM NOVO MUNDO

Artigo apresentado ao curso de graduação em Física da Universidade Católica de Brasília, como requisito parcial para obtenção do Título de Licenciado em Física.

Orientador (a): Dr. Paulo Henrique Alves Guimarães

Brasília – DF
2018

Universidade Católica de Brasília

FOLHA DE APROVAÇÃO TCC

Artigo de autoria de **GABRIEL CARVALHO VELOSO DANTAS** intitulado **Computação Quântica: a possibilidade de um novo mundo**, apresentado como requisito parcial para obtenção do grau de Licenciado em Física da Universidade Católica de Brasília, em 20 de junho de 2018, defendido e APROVADO, pela banca examinadora abaixo assinada:

Prof. Dr. Paulo Henrique Alves Guimarães
LICENCIATURA EM FÍSICA - UCB

Prof. Dr. Claudio Manoel Gomes de Sousa
LICENCIATURA EM FÍSICA - UCB

BRASÍLIA
2018

AGRADECIMENTOS

Agradeço ao meu orientador, Dr. Paulo Henrique Alves Guimarães, por todo seu auxílio na correção e produção, pelo seu tempo gasto e empenho neste trabalho. Agradeço também à Natália Carrijo que me ajudou na construção deste, cedendo de seu tempo e atenção. Aos professores da Universidade Católica de Brasília que fizeram parte desta minha longa caminhada. A toda minha família, amigos e outros, que fizeram parte dessa jornada de forma direta ou indireta.

COMPUTAÇÃO QUÂNTICA: A POSSIBILIDADE DE UM NOVO MUNDO

GABRIEL CARVALHO VELOSO DANTAS, PAULO HENRIQUE ALVES GUIMARÃES

Resumo:

Apresentamos neste trabalho uma revisão bibliográfica sobre os conceitos fundamentais básicos para um entendimento da computação quântica, a qual contém um caráter qualitativo e de divulgação científica. Portanto, concentramos nossos esforços em busca de artigos, livros e notícias, nos atentando aos seus desenvolvimentos históricos e aos fenômenos físicos da mecânica quântica, com o enfoque na união da computação clássica com a computação quântica. Este trabalho é dividido em dois grandes tópicos, os quais são o direcionamento para a construção da computação clássica e para a computação quântica. Mediante a isso, tem em vista a possível utilização deste artigo pelos professores para formulação de uma aula simples ou uma divulgação.

Palavras-chave: Mecânica quântica. Computação Clássica. Computação quântica.

1. INTRODUÇÃO

O tema foi escolhido através de uma curiosidade para entender os conceitos e fundamentos básicos por trás da computação quântica. Após uma longa leitura, pesquisas em artigos e algumas conversas com colegas de curso, ficou clara a baixa divulgação científica e a dificuldade no entendimento dos conceitos básicos que viabilizam a construção da computação quântica.

A computação clássica é, hoje em dia, uma ferramenta indispensável para “qualquer pessoa” em nossa sociedade. Em decorrência de seu desenvolvimento, foi possível a realização do processamento de dados e de trocas de informações em uma velocidade extremamente rápida. Entretanto, para pessoas e empresas que utilizam dessas ferramentas, tornou-se necessário que os dados e as informações fossem mantidos em sigilo e lidos apenas por pessoas as quais têm o interesse em enviar ou receber tais dados ou informações, e, para isso, foi empregado algum tipo de criptografia. Hodiernamente, o sistema de criptografia mais utilizado é assegurado ao protocolo RSA, que se baseia na fatoração de números muito grandes com a finalidade de encontrar dois números primos entre si (um responsável pela criptografia e outro pela chave). Este sistema de segurança trabalha na incapacidade dos computadores clássicos de conseguirem realizar esses cálculos em pouco tempo, podendo levar milhões de anos até encontrarem os resultados.

> Simplesmente não havia uma demonstração matemática rigorosa de que esse algoritmo (capaz de quebrar os códigos gerados por RSA) não existia. Ou seja, a segurança do sistema de comunicação secreta dos computadores clássicos era baseada em uma crença, e não em uma prova científica. (OLIVEIRA; VIEIRA, 2009, p. 139)

A computação quântica vem com a proposta de permitir o processamento de informações em velocidade considerada impossível para um computador clássico (OLIVEIRA; VIEIRA, 2009, p. 8), possuindo os melhores tipos de criptografias (BB84,B92, e outros) baseadas em propriedades quânticas, sendo mais seguros que a criptografia RSA.

No ano de 1994, Peter Shor, trabalhando no laboratório da AT&T, nos Estados Unidos, descobriu um algoritmo quântico notável de fatoração (OLIVEIRA; VIEIRA, 2009, p. 134), nomeado de Algoritmo de Shor, o qual possuía a capacidade de decifrar os dados criptografados pelo sistema RSA com muita eficiência, utilizando propriedades quânticas. A partir disso, as preocupações em torno da descriptografia do sistema RSA foram ampliadas, e, fundamentando-se em tal, as empresas começaram a investir rápido no desenvolvimento de computadores quânticos.

Para facilitar melhor o entendimento desses aspectos apresentados na computação quântica é preciso entender os conceitos físicos que possibilitaram o desenvolvimento da mecânica quântica. É necessário então, entender um pouco e de forma breve os contextos históricos de seu desenvolvimento e os seus pontos de partida.

A mecânica clássica foi marcada pelo determinismo de Isaac Newton, sustentado pelas suas famosas três leis, que condensam uma grande magnitude de fenômenos da mecânica clássica (além da criação do cálculo diferencial e integral, da lei da gravitação universal, entre outros).

> Devemos considerar o estado presente do universo como efeito dos seus estados passados e como causa dos que se vão seguir. Suponha-se uma inteligência que pudesse conhecer todas as forças pelas quais a natureza é animada, e o estado em um instante de todos os objetos - uma inteligência suficientemente grande que pudesse submeter todos esses dados à análise -, ela englobaria na mesma fórmula os movimentos dos maiores corpos do universo, e também dos menores átomos: nada lhe seria incerto e o futuro, assim como o passado, estaria presente ante os seus olhos. (LAPLACE. 1990, apud, SILVEIRA, 1993, p. 138)

Outrossim, com as teorias do físico escocês James Clark Maxwell, foram descritos em seus trabalhos os fenômenos de termodinâmica e do eletromagnetismo. Em uma de suas descrições, conseguiu-se unir um conjunto de quatro equações que descreve com clareza a luz como sendo uma onda eletromagnética.

Os físicos, então, no final do século XIX, acreditavam que todos os fenômenos poderiam ser explicados com as leis da mecânica clássica (Newton) e com o eletromagnetismo (Maxwell), sobrando apenas problemas de aplicações mais específicas. Lord Kelvin (ou William Thomson), físico escocês, chegou a afirmar que “apenas duas nuvens obscureciam o céu cristalino da física”: a primeira nuvem era o problema da velocidade relativa da luz no Éter e a segunda o problema da radiação de um corpo negro. A primeira foi explorada em 1905 pelo físico alemão Albert Einstein, que publicou a teoria da relatividade restrita; em um de seus dois postulados assumia o princípio da constância da velocidade da luz, alegando que a existência do éter luminífero é supérflua, não havendo a existência de um espaço em repouso absoluto (ARRUDA; VILLANI, 1996) (Einstein em seu período de vida também produziu diversos artigos: Efeito Fotoelétrico, Movimento Browniano, Teoria da Relatividade geral etc.). A segunda nuvem veio a ser resolvida por Max Planck,

considerado o pai da teoria quântica, que conseguiu solucionar o problema de radiação de um corpo negro, assumindo que esta seria emitida ou absorvida pelos corpos em pequenos pacotes de energia, denominados de *quantum*. Anos após a ideia de Planck, Einstein propôs que a onda eletromagnética (Luz) era formada pelos pequenos pacotes de energia, e os *quantum* de luz receberam o nome de fótons.

Posteriormente aos trabalhos apresentados, que foram propostas de solução para as duas nuvens que obscureciam o céu cristalino da física, deram-se início os dois novos estudos: a mecânica relativística e a mecânica quântica. Os conceitos e estudos apresentados pela mecânica quântica que tornaram possível a computação quântica são: A dualidade Onda-Partícula; Princípio de complementaridade não excludente; Princípio da incerteza (Equações de Schrödinger); Teoria probabilística (posição/velocidade); Os conceitos de Spin; Equação de Dirac; Paradoxo de EPR (explicado pela teoria de Bell, dando início à ideia de emaranhamento quântico) e entre outros tão importantes quanto esses conceitos muito estranhos para a realidade clássica, pois estas propriedades do estado quântico desaparecem extremamente rápidas quando entram em contato com o meio ambiente.

É também indubitável a necessidade de entendimento dos conceitos básicos da computação clássica e do seu desenvolvimento histórico, passando por seus principais autores, sendo estes, majoritariamente, matemáticos.

> No século XX a humanidade acompanhou um virtuoso desenvolvimento tecnológico, que se refletiu nas mais diversas áreas de conhecimento e setores de atividades. Um fato que muitas pessoas desconhecem é que o grande salto tecnológico dado pelo homem no século passado se apoiou nos dois grandes triunfos intelectuais estabelecidos no mesmo período. As duas grandes dádivas científicas que precederam as descobertas tecnológicas que modificaram o estilo de vida do homem são a Mecânica Quântica e a Ciência da Computação. (MATTIELO et al., 2012)

A teoria da computação e a teoria de informação surgiram de conceitos puramente matemáticos, cujas bases vieram, respectivamente, dos matemáticos Alan Turing e Claude Shannon. O inglês Alan Turing, conhecido como o pai da computação, desenvolveu a noção abstrata de computação programável, conhecida como as máquinas de Turing (popularmente chamadas de computador), cuja principal propriedade é a resolução de problemas matemáticos por algoritmos, que realizam seus cálculos sobre enormes sequências bits (unidades de informação, que podem assumir o valor de 0 ou 1) por meio de portas lógicas. Estas sequências de bits são manipuladas através das operações lógicas que podem modificar, enviar, criptografar ou realizar cálculos, por exemplo.

Tais conceitos foram apresentados como uma união de duas grandes ciências, formando então os computadores clássicos, em que os conceitos matemáticos passaram a ter realidades físicas, como, por exemplo, a passagem ou não de corrente elétrica representando os bits. As portas lógicas capazes de realizar as operações lógicas ganharam realidades físicas por meio de circuitos elétricos formados por transistores, diodos e capacitores, e foram nomeadas de circuitos integrados. Esses circuitos estão ligados à velocidade de processamento e à capacidade de armazenamento que estão associadas, respectivamente a energia e a entropia (OLIVEIRA; VIERA, 2009, p. 107). Por conseguinte, com o desenvolvimento e a sofisticação do estudo de semicondutores, os circuitos passaram a ser cada vez menores.

> No início de 1960, Gordon Moore, um dos fundadores da Intel, com base em suas observações, concluiu de forma empírica que a cada um ano e meio, o número de componentes eletrônicos em um chip dobraria, e por volta de 2020 um bit já seria representado por apenas um átomo. (OLIVEIRA; VIERA, 2009, p.134)

> Já o norte americano Claude Shannon definiu matematicamente o quanto de informação poderia ser enviado por unidade de tempo (bits por segundo) por meio de um canal de comunicação (ruidoso ou não) (OLIVEIRA; VIERA, 2009, p. 113).

Ele, então, criou meios para evitar o ruído (efeito no qual se perde/ corrompe alguma informação) e para codificar, transmitir e recuperar qualquer informação. Essas ideias nortearam o que é conhecido hoje como computação quântica.

Tendo em vista que este será um trabalho de divulgação científica para que pessoas leigas se interessem pelo assunto sem que estas tenham o conhecimento prévio de mecânica quântica ou computação clássica, este artigo apresenta um caráter histórico, passando pelos conteúdos mais relevantes da mecânica quântica e da computação, para que seja possível que professores utilizem dele para a formulação de uma aula simples ou uma divulgação.

2. MATERIAL E MÉTODOS

Esta pesquisa tem um caráter qualitativo e de divulgação científica. Portanto, concentrou seus esforços num trabalho de revisão bibliográfica com enfoque na união da computação clássica e da mecânica quântica, atentando-se aos seus desenvolvimentos históricos e aos fenômenos, com a finalidade de explicar conceitos e fundamentos básicos que viabilizam a construção da computação quântica. As fontes foram analisadas durante a produção do artigo, buscando através dos Títulos e *abstract* em primeira instância. Durante as leituras foram coletados os dados e os conteúdos mais relevantes. Os sites e pesquisas realizadas não se limitaram a apenas um, porém, o mais utilizado para pesquisa foi o “Google acadêmico”.

Este trabalho possui um intuito pedagógico, sendo elaborado com uma linguagem mais simples a fim de facilitar o acesso de uma quantidade maior de pessoas para conhecer o campo fascinante da computação quântica.

3. COMPUTAÇÃO CLÁSSICA

Será feita uma breve introdução à máquina de Turing e seu funcionamento, abordando apenas uma noção intuitiva acerca disso. Sendo este trabalho dividido em duas partes, a primeira sobre computação clássica e a segunda sobre computação quântica.

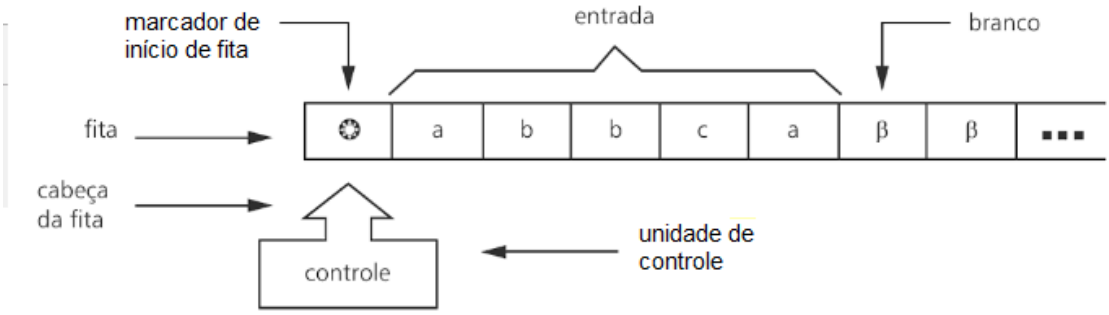
O inglês Alan Turing[1], no ano de 1936, desenvolveu a proposta de um modelo de máquina com um mecanismo bem simples. Este baseava-se na formalização da ideia de uma pessoa fazer cálculos. Entretanto, só após 20 anos foi desenvolvido o primeiro computador digital. Tal máquina é capaz de realizar, através de algoritmos formalizados, o processamento de funções, o reconhecimento de linguagens e as soluções de problemas, os quais podem ser solúveis ou não solúveis, entre outros.

> O ponto de partida de Turing foi analisar a situação na qual uma pessoa, equipada com um instrumento de escrita e um apagador, realiza cálculos em uma fita ou folha de papel organizada em quadrados. (DIVERIO; MENEZES, 2009, p. 133)

Neste ponto de partida de Turing a pessoa realizaria uma sequência de operações simples, como ler e alterar um símbolo de um quadrado e se mover para outro. O trabalho então seria encontrar uma representação satisfatória para viabilizar esse procedimento.

Para a criação de tal máquina essa deveria ser constituída de uma fita “tão grande quanto necessária” para a direita e para a esquerda, usada como o dispositivo de entrada, de saída e de memória de trabalho de forma simultânea; uma unidade de controle, capaz de ler e de gravar (denominada de cabeça da fita), pela qual haveria o acesso às informações gravadas na fita (além de se movimentar para esquerda e direita); e uma função de transição, definida pelo estanho, no qual a máquina comanda as leituras, as gravações e o sentido da movimentação da cabeça.

FIGURA 1 – Fita e unidade de controle de uma máquina de Turing.



Seus ingredientes: (1) Fita, dividida em pequenos quadrados; (2) um alfabeto de símbolos a serem escritos (bits); (3) a cabeça para leitura e gravação; e (4) função de transição responsável pelo comando da cabeça de leitura. Fonte: (DIVERIO; MENEZES, 2009, p.134)

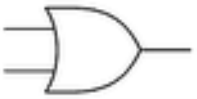
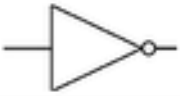
Todos estes ingredientes estão presentes em qualquer computador clássico, atuando nas maravilhas de sons, de imagens, de cálculos e de textos que tornam nossas vidas tão simples e mais divertidas, como a conexão com o mundo por meio da internet e a resolução de problemas matemáticos complexos.

Esse complexo informacional é representado e manuseado nos computadores clássicos mediante as combinações de apenas dois símbolos: o 0 e o 1 (OLIVEIRA; VIEIRA, p. 93). Portanto, denomina-se de Bit (*binary-digit* ou dígito binário) uma unidade de informação (conceito puramente matemático e independe do fato de podermos representá-los como objetos reais) que pode valer 0 ou 1, onde qualquer informe pode ser expresso por sequências desse bit. A cada bit apresentado na combinação, dobra-se o número de possibilidades e consequentemente a representação de novos símbolos. Destarte, é preciso fazer operações lógicas sobre os bits para que se possa manusear, transmitir, gravar e apagar a informação.

Alguns matemáticos descobriram que todos os cálculos matemáticos poderiam ser resolvidos com apenas três operações lógicas elementares sobre bits. Desse modo, essas operações são chamadas de portas lógicas e existem inúmeros

conjuntos dessas elementares, mas os mais comuns são formados por portas, cujos nomes em inglês são *AND* (ou E), *OR* (ou OU) e *NOT* (ou NÃO).

Figura 2- Chaves lógicas elementares.

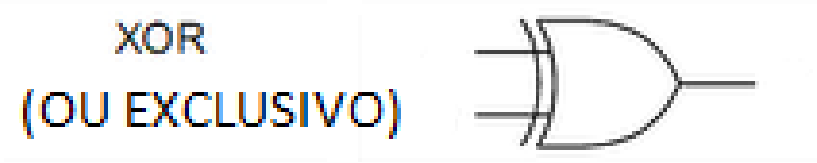
Função Lógica Básica	Símbolo Gráfico da Porta
AND	
OR	
NOT	

Fonte: Elaboração própria.

A porta lógica *NOT* age apenas sobre um bit de cada vez e é responsável pela mudança do valor de entrada, ou seja, quando ele for 0, sairá com o valor de 1 e vice-versa. As outras duas portas lógicas atuam sobre dois bits na entrada e apenas um na saída, podendo se estender a um número qualquer de variáveis. O *AND* realiza a seguinte operação sobre os dois bits de entrada: quando ambos forem 1, sairá com o valor de 1, outrossim, se houver um bit 0, ele sairá com valor 0. O *OR* realiza a operação sobre os dois bits de entrada: quando ambos forem 0, ele sairá 0 e se houver um bit 1, ele sairá com valor 1. Dentre essas operações, a *AND* e a *OR* são irreversíveis, pois existe a perda de informação em sua saída; contudo, a *NOT* é totalmente reversível, pois não existe a perda de informação.

Através da combinação das portas lógicas é possível obter qualquer operação lógica sobre bits- uma das mais importantes é a porta chamada de *XOR* (OU-EXCLUSIVO), que atua sobre dois bits mudando o valor de um deles (denominado Bit-alvo), condicionado a essa alteração pelo valor de outro (bit-controle). Esta é uma operação totalmente reversível, pois entram dois bits e retornam-se os dois alterados na saída.

FIGURA 3- Chave lógica *XOR* (OU EXCLUSIVO)



Fonte: Elaboração própria.

Nem todos os cálculos que um computador consegue resolver são simples ou estão no mesmo patamar de dificuldade. A classificação dessa dificuldade é dada pelo tempo e espaço (memória) necessários para que o melhor algoritmo de resolução possa resolver. Um dos problemas cuja dificuldade é alta, é a fatoração, pois o tempo necessário para a resolução de problemas que envolvem a fatoração cresce de maneira exponencial, de acordo com o número de variáveis do número.

Entretanto, problemas assim têm uma enorme utilidade para o envio de mensagens secretas, chamadas de criptografia.

Os computadores clássicos são associados a sua grande velocidade de processamento em decorrência da miniaturização dos chips pelo estudo de semicondutores, que, portanto, consomem menos energia em decorrência da sua capacidade de memória, que com o passar do tempo poderia desorganizar, por meio das operações lógicas, as informações pelo efeito físico chamado de entropia.

> No início de 1960, Gordon Moore, um dos fundadores da Intel, com base em suas observações, concluiu de forma empírica que a cada um ano e meio o número de componentes eletrônicos em um chip dobraria, e por volta de 2020 um bit já seria representado por apenas um átomo. (OLIVEIRA; VIERA, 2009, p.134)

Naquele momento, então, deu-se início a ideia de um computador quântico.

Em vista disso, os outros conceitos dentro da mecânica quântica e da computação quântica não necessitam de entendimentos prévios, pois serão introduzidos de forma simplificada.

4. COMPUTAÇÃO QUÂNTICA

4.1 A IDEIA DOS Q-BITS.

No ano de 1947, os físicos norte-americanos John Bardeen (1908-91), Walter Brattain (1902-87) e William Shorckley (1910-89) fizeram a descoberta revolucionária na área eletrônica, o primeiro transistor. Já na década de 1960, começaram as discussões em torno da miniaturização da eletrônica. Porém, nessa época não havia muita preocupação com relação a essa redução dos componentes eletrônicos, levando Feynman a comentar, em 1959, numa palestra na Sociedade Americana de Física (APS): “Ainda existe muito espaço lá embaixo” (OLIVEIRA; VIEIRA, 2009, p. 117).

Com a redução dos componentes eletrônicos e o aumento da velocidade e do espaço de memória nos computadores, tornou-se possível que físicos teóricos e engenheiros conseguissem fazer simulações de fenômenos naturais cada vez mais complexas. Entretanto, o computador clássico é macroscópico, sem propriedades inerentes às moléculas, átomos e sub-átomos. Em decorrência disso, para simular sistemas quânticos sem aproximações é necessário um computador quântico.

A primeira ideia de computação quântica surgiu quando Charles Benett descobriu, em 1973, uma computação com base em chaves lógicas totalmente reversíveis (resolvendo um problema da computação clássica). No ano de 1980, Paul Benioff propôs que, sendo os fenômenos quânticos temporariamente reversíveis, esses poderiam ser utilizados para realizar as operações lógicas de Benett (OLIVEIRA; VIEIRA, 2009, p. 121). Diz-se que um fenômeno é irreversível quando pode-se fazer distinção no seu ponto de vista temporal, e reversível quando é impossível diferenciar a sua ordem temporal.

Ressaltando que os Bits são conceitos puramente matemáticos e só podem assumir valores de 0 ou 1, é possível perceber que estes são atuantes em chaves lógicas e mutuamente excludentes que ganham forma física com a passagem ou não de corrente elétrica pelos microchips. De maneira análoga, os Bits Quânticos ou

Q-bits são a unidade de informação quântica muito semelhante aos bits clássicos, conquanto, aqueles podem assumir simultaneamente os dois valores de 0 e 1, pois o estado quântico pode estar superposto.

Na natureza têm-se muitos exemplos de Q-bits, pois qualquer sistema que possua dois estados quânticos bem distintos pode representar 1 q-bit. Um exemplo deste é a polarização de um fóton ou o próprio átomo, através dos níveis de energia ou pelos spins dos núcleos. Os elétrons nos átomos ocupam um orbital ao qual está associada a uma energia do átomo. Considerando-se dois níveis de energia daqueles, podemos associar a um deles o valor lógico de 1 e o outro de 0 (OLIVEIRA; VIEIRA, 2009, p. 124). Desse modo, pode-se criar uma situação onde o elétron ocupe simultaneamente os dois orbitais quânticos, o que corresponde a superposição de 0 e 1. Com essa superposição quântica é possível obter simultaneamente os valores de 0 **e** 1; em contrapartida das operações clássicas em que obtém-se 0 **ou** 1.

4.2 ALGUMAS OPERAÇÕES LÓGICAS.

Para se montar uma computação, seja ela clássica ou quântica, é necessária a construção de chaves lógicas. As chaves lógicas quânticas devem atuar sobre os q-bits para executar uma operação lógica. Ademais, o hardware de uma chave lógica depende da representação dos q-bits que se usa.

Existem semelhanças entre chaves lógicas clássicas e quânticas, outrossim, há diferenças importantes, como, por exemplo, as chaves quânticas são sempre reversíveis, enquanto as clássicas podem ser tanto reversíveis (como a NOT) quanto irreversíveis (como a AND e a OR), além disso, há chaves quânticas que não tem análogo clássico, como a chamada “operação Hadamard” ou “Chave Hadamard”, em homenagem ao matemático francês Jacques Hadamard.

A Chave de Hadamard, ao atuar sobre 1 q-bit no estado 0, coloca-o em uma superposição de 0 e 1. Como o fenômeno da superposição de estados lógicos não existe classicamente, caso essa chave lógica atue em um número qualquer de q-bits, como N, por exemplo, esta criaria uma superposição de todas as 2^n combinações possíveis. Por meio disso, nota-se que num computador quântico todos os estados lógicos possíveis são manipulados simultaneamente e tal chave pode ser aplicada só a uma parte dos q-bits (FREITAS; CUNHA, 2010).

Caso haja uma combinação das chaves Hadamard e XOR, será possível criar uma importante operação lógica em computação quântica, pois esta gera um estado de emaranhados em um circuito quântico.

> Observem agora, senhores, um desdobramento interessante: se uma medida for feita sobre o primeiro q-bit desse estado, haverá 50% de chance de encontramos 0 e 50% de chance de encontrarmos 1. Suponha que se encontre 0. Isso quer dizer que o estado do segundo q-bit também será 0, mesmo que nenhuma medida tenha sido feita sobre ele. Mas, se em vez de 0 encontramos 1 na medida do primeiro, o estado do segundo também vai para 1. Ou seja, a medida sobre o primeiro q-bit influencia o estado do segundo q-bit. (OLIVEIRA; VIEIRA, 2009, p. 128)

No campo da computação quântica, a primeira grande reviravolta se deu perto do final do século XX, mais especificamente em 1985. Naquele ano, apareceu

o que é considerado o primeiro algoritmo quântico em um artigo assinado por David Deutsch, físico da Universidade de Oxford (OLIVEIRA; VIEIRA, 2009, p. 130).

O algoritmo seria como se você pudesse verificar uma moeda dos dois lados em apenas uma observação, mas sua descrição completa é muito técnica para o propósito desse artigo. Conquanto, é fato que esse algoritmo torna as operações muito mais rápidas que as operações clássicas, e este só é possível ser implementado devido a utilização do fenômeno de superposição.

4.3 O ALGORITMO DE PETER SHOR

A criptografia é a arte da comunicação secreta. A ideia desta é enviar uma mensagem secreta de um ponto a outro, sendo possível a leitura apenas por quem recebe e por quem envia. A pessoa que recebe precisa descodificar a mensagem para ser lida. O sistema de criptografia responsável por garantir a segurança dos cartões de crédito é o sistema RSA (em homenagem aos seus inventores Ron Rivest, Adi Shamir e Len Adleman) (SILVA; PAPANI, 2018)

> A possibilidade de comunicação entre computadores pela internet trouxe novos desafios para a criptografia. Por ser relativamente fácil interceptar mensagens enviadas por linha telefônica, torna-se necessário codificá-las, sempre que contenham informações sensíveis, como transações bancárias ou comerciais, ou até mesmo uma compra feita com cartão de crédito. (SILVA; PAPANI, 2018, p. 6)

O sistema RSA é baseado na incapacidade matemática de um computador não conseguir fatorar números muito grandes. Ou seja, baseia-se na crença de que um computador levaria um tempo quase infinito para solucionar este problema, e não em uma prova científica (OLIVEIRA; VIEIRA, 2009, p. 134).

> No início da década de 1990 ficou claro que o emaranhamento pode ser encarado como um recurso disponível na Natureza, assim como a energia, e que pode ser utilizado para se executar de maneira muito eficiente algumas tarefas computacionais [22, 23] e informacionais [11, 12, 24]. (RIGOLIN, 2008, p. 7)

No ano de 1994, Peter Shor, trabalhando nos laboratórios da AT&T (nos EUA), descobriu um algoritmo quântico notável: um algoritmo de fatoração. Essa descoberta fez com que o interesse da comunidade científica aumentasse pela computação quântica. O algoritmo de Shor é capaz de decifrar as mensagens criptografadas pelo RSA (VENITES FILHO; PRADO, 2014). É importante enfatizar que o segredo por trás deste algoritmo são os fenômenos quânticos de emaranhamento e superposição.

Além da sua importância, representa um verdadeiro desafio a Tese forte de Church-Turing, pois é a primeira evidência que os computadores quânticos são inerentemente mais poderosos (VENITES FILHO; PRADO, 2014).

Em princípio, os computadores clássicos também poderiam fatorar um número grande, mas necessitaria de um tempo consequentemente maior, cerca de

milhões de anos. Portanto, este problema só poderia ser resolvido exclusivamente por um computador quântico em tempo polinomial no número de dígitos do número (FREITAS; CUNHA, 2010).

Outros grandes avanços na computação quântica aconteceram também na Criptografia quântica (BB84,B92, e outros) e na transmissão de informações com a utilização dos fenômenos de superposição e emaranhamento.

5. CONCLUSÕES

A história da computação quântica na física percorreu caminhos distintos e muito interessantes. Inicialmente na física, saindo do determinismo de Newton e de Maxwell, entrando por meados do final do século 20 na Mecânica quântica, a qual devastou a ideia determinista e do nosso “senso comum”. E que, posteriormente, se uniu com os conceitos matemáticos da computação clássica, os quais, hoje em dia, são indispensáveis para a nossa sociedade, mas que surgiram com alguns “problemas” em torno da criptografia RSA, com o desenvolvimento do algoritmo de Peter Shor. Esse que utiliza-se de propriedades quânticas como a superposição e o emaranhamento para descriptografar o sistema RSA, mostrando assim o poder dos computadores quânticos com uma capacidade de processamento de informações em velocidades consideradas impossíveis.

Com o passar do tempo esta área da ciência vem mostrando cada vez mais algoritmos quânticos e novas maneiras de processar informações consequentemente mais eficientes, mostrando o quão promissor pode ser para os novos pesquisadores.

Quantum Computation: The possibility of a new world

ABSTRACT:

We present in this work a bibliographical review about the basic concepts and fundamentals for an understanding about Quantum Computation. Considering that this is a work of scientific divulgation for lay people to be interested in the subject without necessity of prior knowledge in quantum mechanics or in classical computation. The aim of this article is to present an introductory text for teachers that are interested in formating a simple lesson or in disseminate of scientific discoveries.

Keywords: Quantum Mechanics, Classical Computing, Quantum Computation.

.

REFERÊNCIAS

ARRUDA, S. M.; VILLANI, A. Sobre as origens da relatividade especial: Relações entre quanta e relatividade em 1905. **Caderno Catarinense de Ensino da Física**, v. 13, n. 1, p. 32–47, 1996. Disponível em: <http://www.periodicos.ufsc.br/index.php/fisica/article/view/7077/6548>.

CABRAL, G.;LIMA, A.; LULA JR, B. Interpretando o algoritmo de Deutsch no interferômetro de Mach-Zehnder. **Revista Brasileira de Ensino de Física**, v. 26, n. 2, p. 109 - 116, (2004). Disponivel em : <www.sbfisica.org.br>.

DIVERIO, T; MENEZES, P. **Teoria da computação:** Máquinas Universais e Computabilidade. Cap 5: Maquinas de Turing, 3.Ed, Bookman Editora, 2009. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=459EInmoh2cC&oi=fnd&pg=PR1&dq=maquina+de+turing+algoritmo&ots=hqxcYv4xUM&sig=oo7xKYEs_GzDCTsPDDBvg3zaR4A#v=onepage&q=maquina%20de%20turing%20algoritmo&f=false>.

FREITAS, A.; Cunha, M. **Algoritmo de Shor e sua aplicaçao à fatoraçao de números inteiros.** UFMG, 2010. Disponível em: < http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/EABA-85FJXP/dissertacao_adrianaxavier.pdf?sequence=1>.

MATTIELO, F./et al. Decifrando a Computação Quântica. **Caderno de física do UEFS**, v. 10, p. 31–44, 2012. Disponível em: <http://dfis.uefs.br/caderno/vol10n12/a4MattielCQuantica.pdf> Acesso em 6 jun. 2018.

OLIVEIRA, Ivan ; VIEIRA, Cassio Leite. **A revolução dos q-bits:** O admirável mundo da computação quântica. Editora Zahar, 2009.

RIGOLIN, G. Emaranhamento Quântico. Rio de Janeiro: Campinas, n.7 **Revista Physicæ,** 7. Unicamp, 2008. Disponível em: <https://physicae.ifi.unicamp.br/index.php/physicae/article/view/physicae.7.1/47>.

SILVA, F.; PAPANI, F. **Um pouco da história da criptografia.** In: SEMANA ACADEMICA DA MATEMATICA, 22. Paraná: Unioeste. Disponível em: < http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16> acesso em 6 de jun. 2018.

SILVEIRA, F. L. da. Determinismo, Previsibilidade e Caos. **Caderno Catarinense de Ensino de Física**, v. 10, n. 2, p. 137–147, 1993. Disponível em: <https://www.if.ufrgs.br/~lang/Textos/Determinismo_previsibilidade_caos.pdf>. Sequência de resumos, mas de uma análise articulada, crítica e reflexiva do próprio aluno, sobre o que já foi escrito a respeito do assunto.

VENITES FILHO, E.; PRADO, S. **Algoritmo de Shor para fatoração de inteiros.** In: Salão de Iniciação Científica,26. Campos do vale.2014-UFRGS. 2014. Disponível em:< http://www.lume.ufrgs.br/handle/10183/112979> Acesso em: 6 jun. 2018.

Campus I - QS 07 – Lote 01 – EPCT – Águas Claras – Brasília – DF CEP: 71966-700 - (61) 3356-9000
Campus Avançado Asa Norte - SGAN 916 Módulo B Avenida W5 - CEP: 70790-160 - Brasília/DF - Telefone: (61) 3448-7134
Campus Avançado Asa Sul - SHIGS 702 Conjunto 2 Bloco A - CEP: 70330-710 - Brasília/DF - Telefone: (61) 3226-8210