SIMULAÇÕES COMPUTACIONAIS DOS ALGORITMOS QUÂNTICOS ATUAIS APLICADOS À PRIVACIDADE DAS COMUNICAÇÕES

Victor Biral do Nascimento Plácido – biral.victor@gmail.com
Vinicius Fernandes dos Santos Silva – vinifersil@gmail.com
Prof. Dr. Antonio Newton Licciardi Junior (Orientador) – newton.licciardijr@gmail.com

RESUMO

A computação quântica é uma tecnologia que vem ganhando espaço nos últimos anos em pesquisas e implementações práticas. Grandes empresas como a IBM e a Microsoft têm investido recursos na criação de um computador quântico viável. Uma vez que o desenvolvimento da computação quântica atingir o patamar de viabilidade tecnológica (custo x benefícios), pesquisadores e projetistas da área de computação clássica poderão considerar a inserção nesse novo modelo. O corrente documento apresenta os paradigmas da computação quântica, tendo a criptografia quântica como objeto de estudo. Os conceitos básicos de mecânica quântica necessários para o tema são explanados a partir de sua aplicação prática na computação quântica. Os algoritmos de criptografia quântica atuais e viáveis são explorados teórica e praticamente, dentre estes o BB84 (BENNETT, BRASARD, 1984) e o E91 (EKERT, 1991), que são protocolos de QKD (Quantum Key Distribution).Estabelece-se, através de simulações, um modelo prático de aplicação do protocolo BB84. Resultados estatísticos são apresentados, demonstrando a capacidade de efetuar a distribuição de chave criptográfica de algoritmos simétricos de forma segura e robusta.
Palavras-chave: Computação Quântica. Criptografia Quântica. QKD (Quantum Key Distribution).

COMPUTATIONAL SIMULATIONS OF CURRENT QUANTUM ALGORITHMS APPLIED TO PRIVACY OF COMMUNICATIONS

ABSTRACT

Quantum computing is a technology that has been gaining ground in recent years in research and practical implementations. Big companies like IBM and Microsoft have invested resources in creating a viable quantum computer. Once the development of quantum computing reaches the level of technological feasibility (cost x benefits), researchers and designers of the classical computing area may consider the insertion in this new model. The current document presents the paradigms of quantum computation, with quantum cryptography as the object of study. The basic concepts of quantum mechanics needed for the theme are explained from its practical application in quantum

computation. The current and feasible quantum cryptography algorithms are theoretically and practically exploited, among them the BB84 (BENNETT, BRASARD, 1984) and E91 (EKERT, 1991), which are QKD (Quantum Key Distribution) protocols. It is established, through of simulations, a practical model of application of the BB84 protocol. Statistical results are presented, demonstrating the ability to perform cryptographic key of symmetric algorithms distribution in a secure and robust manner.
Keywords: Quantum Computation. Quantum Cryptography. QKD (Quantum Key Distribution).

1 INTRODUÇÃO

Na Era Digital que se iniciou no final do Século XX (KLAUS, 2016) são importantes e relevantes os trabalhos que viabilizam melhorias ou novas propostas de criptografia de comunicação em redes públicas ou privadas, com o objetivo de minimizar a possibilidade de que incidentes de segurança não sejam concretizados como vazamentos de informações em comunicações.

A criptografia quântica é um afluente da criptografia que utiliza princípios da Mecânica quântica para garantir o sigilo de uma mensagem. Tais princípios são oriundos do Princípio da Incerteza de Heisenberg (NÚÑEZ, NEVES, 2003) (HEISENBERG, 1927) enunciado pelo físico Werner Heisenberg. em 1927.

Segundo Heisenberg, toda tentativa de medição de parâmetro mencionado uma partícula gera um distúrbio, que pode ser provocado por um simples fóton emitido pelo instrumento de medição, por exemplo. Tal interação foi explicada por De Broglie (1927), na qual postulou que a solução de uma equação de onda de matéria deveria admitir duas soluções, sendo uma delas probabilística. O fóton interfere então no comportamento de uma partícula, como por exemplo um elétron (NÚÑEZ, NEVES, 2003) tornando impossível precisar absolutamente, como na física clássica, grandezas que permitem definir o estado de uma partícula, senão probabilisticamente. A Criptografia idealizada a partir de princípios quânticos, torna impossível então e determinação da chave da criptografia sem a alteração/destruição da mensagem cifrada por um atacante (TEJA, 2007). Ou seja, pode-se dizer que o processo é intrinsicamente seguro.

O lançamento do Qutip/Python (JOHANSSON, NORI; 2012) e outros simuladores viabilizaram, a partir de 2012, o estudo da computação baseada em princípios quânticos. E mais recentemente, o aumento de investimento em P&D em processadores quânticos, realizado por empresas como Google, IBM e Microsoft, tem incrementado oportunidades/diversidade de aplicações e pesquisas.

Pretende-se no corrente trabalho, encontrar simulação (ou computação) viável dos algoritmos quânticos teóricos atuais de criptografia (apresentados na Seção 5.), de forma a cifrar com sucesso um sistema transmissor/receptor.

Para tal, estuda-se o estado atual da computação quântica, de simuladores computacionais e processadores. Além disso, explana-se a proposta de criptografia quântica e viabilidade do estudo de caso em um modelo de comunicação, a fim de garantir a privacidade. Para tal, estuda-se e se escolhe a melhor alternativa de simulador computacional viável, uma vez que o acesso e um computador com processador quântico não é simples de ser obtido no momento. Algumas dessas plataformas estão listadas a seguir:

- *Forest SDK*, uma biblioteca desenvolvida pela Rigetti, que integra uma liguagem de programação, o pyQuil, uma máquina virtual para simulação e um computador quântico (SMITH, CURTIS, ZENG, 2016).
- *Qutip*, um *framework* (método de trabalho) genérico escrito na linguagem de programação Python para simulações numéricas e computacionais de sistemas quânticos abertos e fechados (JOHANSON et al, 2013).
- *IBM Q Experience*, um ambiente de simulação e execução de algoritmos quânticos em um computador quântico de 5 Qubits (SANTOS, 2017).
- *Cirq*, um *framework* desenvolvido pela Google para a simulação e execução de algoritmos NISQ, (Algoritmo Quântico de Escala Intermediária com Ruído) em processadores quânticos. (HO, 2018).
- *Microsoft Quantum*, a plataforma de desenvolvimento quântico da Microsoft, sendo encabeçado pelo desenvolvimento de um computador quântico e de uma linguagem de programação própria, o Q#, que faz com que o computador quântico atue como um coprocessador (SVORE et al, 2018).
- *D-Wave Leap*, é a plataforma desenvolvida pela D-Wave, sendo a primeira empresa voltada exclusivamente para a computação quântica (DWAVE, 2018).

1.1 ESTRUTURA DO TRABALHO

Este trabalho estará estruturado em dez seções:

- A Seção 2 fornece os princípios de mecânica quântica necessários à compreensão dos algoritmos utilizados em computação quântica, bem como os princípios da computação quântica;
- Na Seção 4 explica-se sobre a computação quântica e suas diretrizes;
- Na Seção 5 é realizada uma análise das plataformas de simulação e execução de algoritmos quânticos existentes;
- Na Seção 6 são apresentados os principais algoritmos de criptografia quântica;
- Na Seção 7 a metodologia de pesquisa é discutida;

- Na Seção 8, os resultados estatísticos da simulação são então disponibilizados para discussões;
- A Seção 9 aborda a discussão dos resultados da pesquisa prática;
- A Seção 10 efetua uma breve síntese do caminho trilhado ao longo do trabalho e as conclusões mais relevantes.

2 METODOLOGIA

Com o intuito de analisar o tema proposto, o corrente trabalho foi inicialmente focado no estudo de caso, entendimento e descrição sumária do estado da arte da computação quântica.

Foram analisadas as plataformas disponíveis para simulação e execução de programas de computação quântica pela nuvem afim de escolher a mais viável.

Os algoritmos de criptografia quântica foram analisados de forma a escolher um para utilização entre os principais algoritmos postulados.

Definidas as ferramentas e algoritmos para execução do projeto, foi feito um estudo de caso definido pela cifragem quântica de um sistema de comunicação (transmissor, canal e receptor). O estudo consiste no processo de distribuição de uma chave secreta a partir de um canal quântico, obtendo informações estatísticas sobre a viabilidade do processo.

Os resultados obtidos a partir dos testes basearam a definição do estágio de desenvolvimento atual da criptografia quântica

De acordo com os resultados obtidos, definimos, quais as contribuições para prováveis interessados em pesquisar o tema de criptografia quântica. É também intuito do projeto estabelecer base referencial para desenvolvimento de pesquisas posteriores e contribuir para o estudo de aplicação em mais ampla escala de algoritmos quânticos em proteção de privacidade.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 PRINCÍPIOS DE MECÂNICA QUÂNTICA

Até o presente momento, este documento apresentou a computação quântica como uma evolução natural e viável para a computação. Entretanto, para dar continuidade aos objetivos deste trabalho, a explicação de certos conceitos de mecânica quântica será necessária.

Nesta Seção, os conceitos básicos da mecânica quântica necessários ao entendimento da execução de projetos em computação quântica serão introduzidos.

É importante lembrar que este documento não tem por objetivo demonstrar teorias completas da mecânica quântica, portanto, os conceitos desta Seção foram deliberadamente simplificados e direcionados ao entendimento do processo de QKD que baseia este projeto.

3.1.1 Notação de dirac

De acordo com David A. B. Miller (MILLER, 2008), o estado quântico de uma partícula pode ser descrito como uma lista de números. Esta lista de números pode ser escrita na forma de um vetor, chamado de vetor de estado.

A notação bra-ket de Dirac é utilizada na mecânica quântica para representar os estados da partícula bem como sua evolução.

Em computação quântica, as representações de qubits, registradores e definições de saída de portas quânticas são feitos a partir desta notação.

A expressão $|f(x)\rangle$ é chamada de ket, que é um vetor coluna correspondente a uma função $f(x)$.

Na aplicação da notação em sistemas práticos, Miller explica que dado o processo estatístico de medição de um ket $|\psi\rangle$, podemos definir $|\psi\rangle$ por:

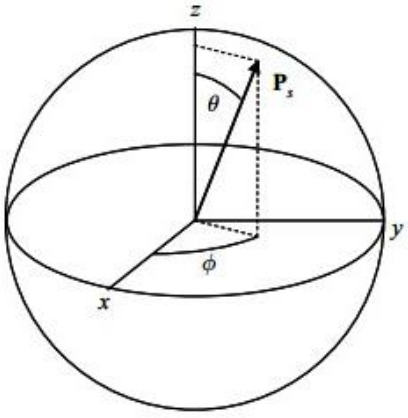
$$|\psi\rangle = \sum_n \alpha_n \, |\psi_n\rangle \qquad (1)$$

Onde α_n é a amplitude de probabilidade de uma base $|\psi_n\rangle$. O que significa que $|\psi\rangle$ tem uma probabilidade $\|\alpha_n\|^2$ de ser medido com o valor $|\psi_n\rangle$.

3.1.2 Esfera de bloch

Uma outra forma de visualização de sistemas quânticos, foi apresentada pelo físico Felix Bloch. A esfera de Bloch representa de forma gráfica a posição polar dos vetores de um sistema com raio unitário. (MILLER,2008, p.303)

Figura 1 - Esfera de Bloch



Fonte: Miller (2008, p. 304)

A Equação 2 (MILLER, 2008, p. 304) descreve o vetor $|s\rangle$ em função de θ e ϕ, ângulos demonstrados na Figura 1.

$$|s\rangle = \cos\left(\frac{\theta}{2}\right)|\uparrow\rangle \; + e^{i\phi} \sin\left(\frac{\theta}{2}\right)|\downarrow\rangle \qquad (2)$$

De acordo com a Equação 2, os vetores definidos por uma função real se situam no plano XZ na esfera de Bloch e os definidos por uma função complexa possuem um valor de Z.

Em computação quântica, a esfera de Bloch se mostra uma ferramenta útil na análise da ação das portas quânticas.

3.1.3 Sobreposição

P.A.M. Dirac, define sobreposição como o fato de que todo estado quântico pode ser representado por uma soma (sobreposição) de outros estados (DIRAC, 1948). Isso significa que cada partícula de dimensões quânticas não é definida por um estado ou outro, mas uma combinação de todos os estados possíveis ao mesmo tempo.

Esse conceito é traduzido para a computação quântica como demonstrado na equação de Dirac par um qubit.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (3)$$

Onde o ket $|\psi\rangle$ é dado pela superposição de $|0\rangle$ com amplitude de probabilidade α e $|1\rangle$ com amplitude de probabilidade β.

A partir desta Equação o qubit pode ser definido não por um valor fixo, como um bit que assume os valores de 1 ou 0, mas por uma combinação probabilística de ambos os valores. De tal forma que ele pode assumir os valores $|0\rangle$, $|1\rangle$ e $\alpha|0\rangle + \beta|1\rangle$.

3.1.4 Emaranhamento

Outro princípio que pode ser utilizado em QKD é o do emaranhamento (Miller, 2008). Este princípio fornece a ideia de que duas partículas em um mesmo espaço de Hilbert podem assumir um comportamento relacionado. A medição do estado de uma partícula altera, portanto, as amplitudes para medição do estado de outra partícula.

Entende-se por espaço de Hilbert, o sistema físico que contém os vetores de estado das partículas em questão.

Pode-se exemplificar este fenômeno com o paradoxo postulado por Einstein, Podolsky e Rosen, demonstrado por Miller a partir da polarização horizontal $|H\rangle$ ou vertical $|V\rangle$ de um fóton.

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2) \quad (4)$$

Significando que caso o fóton 1 seja medido na polarização horizontal, o fóton 2 tem sua amplitude em $|H\rangle_2$ aumentada de $\frac{1}{\sqrt{2}}$ para 1.

Este princípio é utilizado no protocolo E91 de QKD, discutido na Seção 5.2.

3.1.5 Não clonagem

O teorema enunciado por Wootters e Zurek comprova que é impossível fazer uma réplica exata de um sistema com estados aleatórios. (WOOTTERS, ZUREK,1982)

Este teorema tem grande importância em processos de QKD pois todos os processos se baseiam no fato de que seria impossível definir as amplitudes de um bit quântico sobreposto.

Caso houvesse a possibilidade de clonar um bit quântico que é o equivalente a uma partícula, seria possível clona-lo múltiplas vezes e medir todos paralelamente, obtendo todas as amplitudes de probabilidades possíveis.

3.2 COMPUTAÇÃO QUÂNTICA

Como dito anteriormente, uma vez que a miniaturização de componentes de um processador atinja a escala atômica, as leis da física clássica deixarão de valer. Portanto, computadores quânticos vêm a ser aqueles que trabalham em um nível em que acontecem os fenômenos quânticos. (CHOU, KUO, 2009)

A diferença básica entre um computador clássico e um computador quântico é sua unidade de informação. Para um computador clássico, essa unidade é o bit, que assume os valores um ou zero. Na computação quântica, temos o qubit, ou, bit quântico. O qubit pode assumir, assim como o bit, os valores, zero ou um, porém pode ser também uma sobreposição de 0 e 1 (VIGNATTI et al, 2004)

A sobreposição é um princípio fundamental da mecânica quântica que define que uma partícula de dimensões quânticas existe parcialmente em todos os estados possíveis antes que ela seja medida. Desta forma, um qubit sobreposto assume a forma de uma função probabilística de bases zero e um, definida pela notação de Dirac.

As considerações a seguir serão baseadas nos aspectos de como a mecânica quântica suporta os fenômenos computacionais. Portanto o foco da Seção não é a física, mas sua aplicação na computação.

3.2.1 Portas Quânticas

Assim como a manipulação de bits na computação clássica é dado pelo uso de portas lógicas, as portas quânticas executam o mesmo papel em computação quântica.

As portas lógicas quânticas são dadas por matrizes unitárias reversíveis. Isso significa que a matriz que compõe uma porta quântica multiplicada pela sua transposta resulta em sua própria matriz. De tal forma que, na ausência de medições, o bit que passou por uma porta quântica pode ser recuperado. Portanto, todas as portas quânticas são reversíveis, e são inversas de si mesmas (VIGNATTI et al, 2004).

É necessário explicar que o processo de medição aplicado a um qubit no estado de sobreposição resulta na quebra desta sobreposição, portanto impede a reversão de uma porta quântica.

Foram identificados três tipos de porta quântica com maior utilização. A porta de Hadamard cuja principal função é colocar um qubit em sobreposição. A porta CNOT, utilizada para emaranhar

dois bits. E as portas de Pauli que rotacionam o qubit nos eixos da esfera de Bloch. Suas especificações são detalhadas nas seções de 5.1.5 a 5.1.7.

As portas quânticas de rotação de qubits na esfera de Bloch são chamadas de Portas de Pauli porque suas propriedades se dão de acordo com as matrizes de Pauli (MILLER, 2008, p.302), que ocorrem na equação de Pauli que descreve a influência de um campo eletromagnético externo no spin de uma partícula.

3.2.1.1 Matrizes de Portas Quânticas

Toda porta quântica pode ser definida por uma matriz quadrada cujo tamanho é duas vezes o número de entradas da porta.

Dado um registrador $|\psi\rangle$ que representa o conjunto resposta desta porta quântica, para uma combinação de entradas, as colunas da matriz serão compostas pela amplitude de cada componente deste registrador. As bases do registrador $|\psi\rangle$ são dadas na ordem do numeral binário bem como a disposição das colunas da matriz.

Uma matriz de uma porta quântica de duas entradas, por exemplo, seria definida da seguinte maneira:

Dado o registrador $|\psi\rangle_{xy} = \alpha_{xy}|00\rangle + \beta_{xy}|01\rangle + \gamma_{xy}|10\rangle + \delta_{xy}|11\rangle$ que representa o conjunto resposta da porta exemplo, a matriz da porta é dada por:

$$\begin{pmatrix} \alpha_{00} & \alpha_{01} & \alpha_{10} & \alpha_{11} \\ \beta_{00} & \beta_{01} & \beta_{10} & \beta_{11} \\ \gamma_{00} & \gamma_{01} & \gamma_{10} & \gamma_{11} \\ \delta_{00} & \delta_{01} & \delta_{10} & \delta_{11} \end{pmatrix} \quad (5)$$

3.2.1.2 Porta de Hadamard

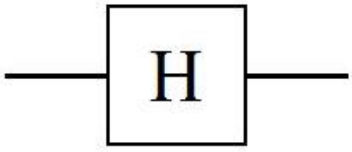
Segundo Vignatti, et al (2004), a porta de Hadamard atua em um qubit, de forma a gerar uma sobreposição. mapeando-o de $|0\rangle$ para $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e de $|1\rangle$ para $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Esta porta é representada pela matriz:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (6)$$

Sua simbologia gráfica é dada pela Figura 1.

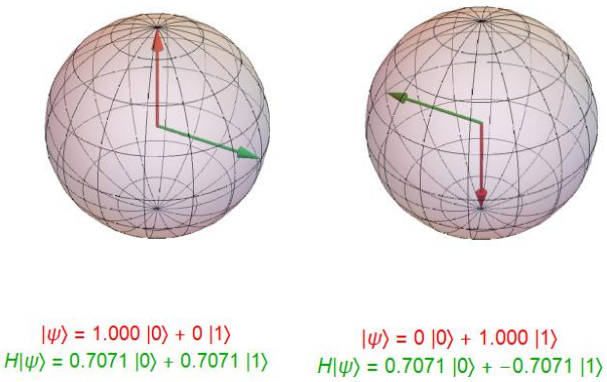
Figura 2 - Representação da Porta de Hadamard



Fonte: Cardonha, De Carli Silva, Fernandes (2005)

A representação da ação da porta de Hadamard nos qubits $|0\rangle$ e $|1\rangle$ é dada na Figura 2.

Figura 3 - Representação da porta de Hadamard na esfera de Bloch



Fonte: Blinder (2017)

3.2.1.3 Porta CNOT

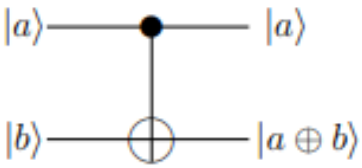
As portas iniciadas com um "C" são portas controladas. As portas controladas têm um qubit de controle e um qubit alvo, alterando o qubit alvo de acordo com o qubit de controle. A porta CNOT inverte o valor do qubit alvo caso o qubit de controle seja $|1\rangle$, caso contrário, nada acontece.

Esta porta é representada pela matriz:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (7)$$

Sua simbologia gráfica é demonstrada a seguir:

Figura 4 - Porta CNOT representada em um circuito Quântico



Fonte: Vignatti et al (2004)

A porta CNOT é comparável a uma porta de disjunção exclusiva clássica, comumente chamada de ou exclusivo. Esta porta tem como saída um bit 1 somente quando as entradas são diferentes a saída é zero. A diferença entre as duas é que, como demonstrado na Figura 4, CNOT tem duas saídas, sendo que o qubit de controle é uma delas.

3.2.1.4 Porta de Pauli-X ou NOT quântica

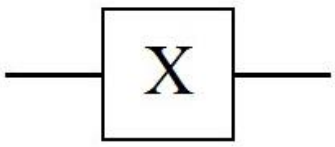
A porta quântica de Pauli-X executa a rotação de um qubit no eixo X da esfera de Bloch. Isto significa que a porta NOT quântica opera da mesma forma que a clássica, ou seja, $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$.

Esta porta é representada pela matriz:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (8)$$

Sua simbologia gráfica é demonstrada a seguir:

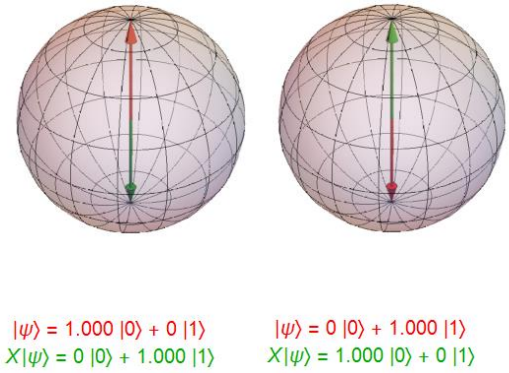
Figura 5 - Representação da porta X



Fonte: Cardonha, De Carli Silva, Fernandes (2005)

A representação da ação da porta de Pauli-X nos qubits 0 e 1 é dada na Figura 5.

Figura 61 - Representação da porta X na esfera de Bloch



Fonte: Blinder (2017)

3.2.1.4 Porta de Pauli-Y

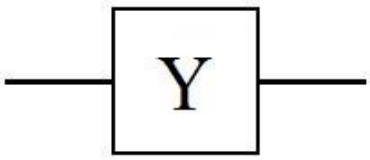
A porta quântica de Pauli-Y atua em um qubit resultando no equivalente a rotacionar o qubit em 180 graus no eixo y da esfera de Bloch. Isso implica em dizer que $Y|0\rangle = i|1\rangle$ e $Y|1\rangle = -i|0\rangle$.

Ela é representada pela matriz:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (9)$$

Sua simbologia gráfica é demonstrada a seguir:

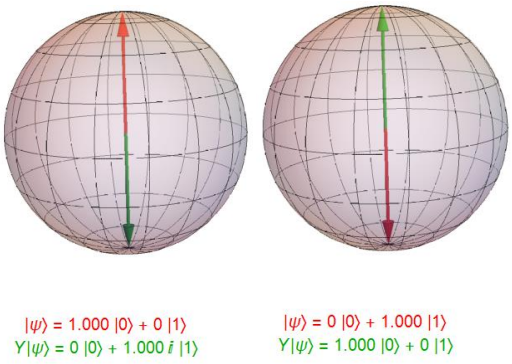
Figura 7 - Representação da porta Y



Fonte: Cardonha, De Carli Silva, Fernandes (2005)

A representação da ação da porta de Pauli-Y nos qubits 0 e 1 é dada nas Figura 8.

Figura 8 - Representação da porta Y na esfera de Bloch



Fonte: Blinder (2017)

3.2.1.4 Porta de Pauli-Z

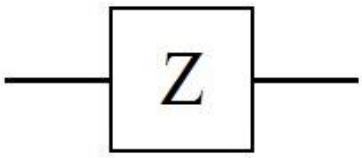
A porta quântica de Pauli-Z atua em um qubit obtendo o resultado equivalente a uma rotação de 180 graus no eixo Z. Isso implica dizer que $Z|0\rangle = |0\rangle$ e $Z|1\rangle = -|1\rangle$.

Ela é representada pela matriz:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (10)$$

Sua simbologia gráfica é demonstrada a seguir:

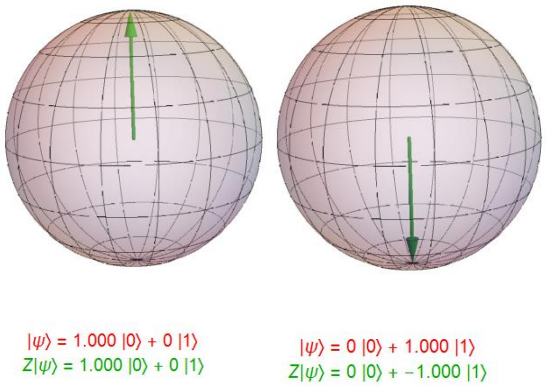
Figura 9 - Representação da porta Z



Fonte: Cardonha, De Carli Silva, Fernandes (2005)

A representação da ação da porta de Pauli-Z nos qubits 0 e 1 é dada nas Figura 10.

Figura 10 - Representação da porta Z na esfera de Bloch



Fonte: Blinder (2017)

4 PLATAFORMAS DE SIMULAÇÃO QUÂNTICA EXISTENTES

Existem pelo menos 40 plataformas existentes na internet que realizam tarefas de simulação de algoritmos quânticos, (FINGERBUTH, 2019). Mas apenas algumas plataformas tem a capacidade de rodar em computadores quânticos reais.

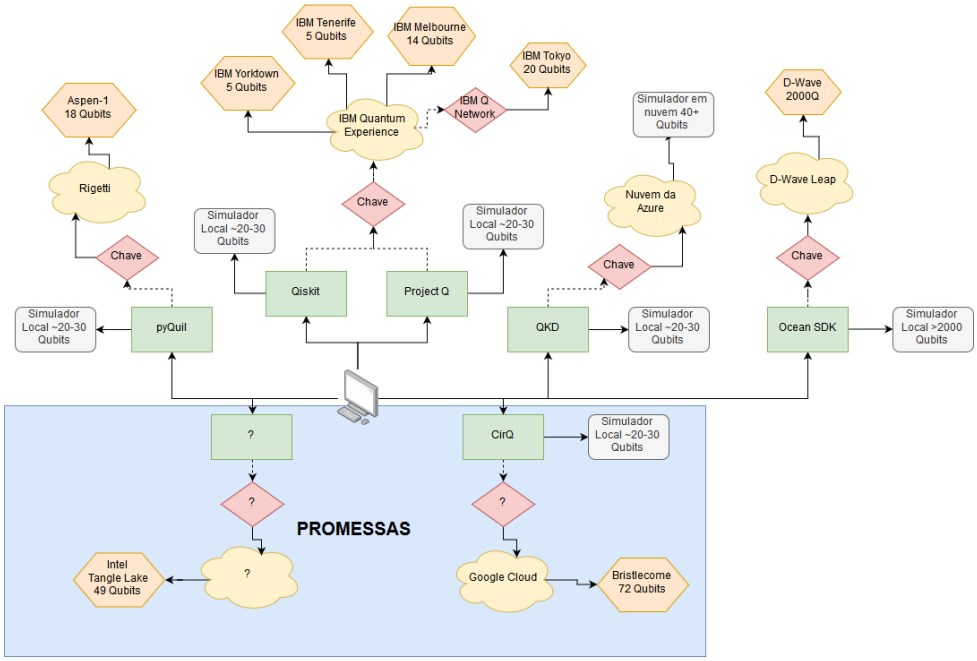
LaRose (2019) lista e explana sobre algumas das seguintes plataformas:

- Forest (pyQuil) da Rigetti;
- Qiskit da IBM;
- ProjectQ;
- Quantum Developer Kit (QDK) da Microsoft.

Acreditamos que também seja interessante citar a plataforma Cirq, por ter como mantenedor o Google, mesmo não tendo um computador quântico disponível ao público nem comentado muito sobre evoluções no processo de desenvolvimento nos últimos meses.

Sabendo ainda que a Intel divulgou que conseguiu produzir uma versão de testes de um processador quântico de 49 Qubits (INTEL 2019), temos o seguinte mapa da tecnologia atual:

Figura 21 - Mapa da tecnologia atual de plataformas quânticas



Fonte: Os autores

Podemos interpretar esta imagem de acordo com as cores dos blocos:

- Verde: Frameworks/Linguagens quânticas utilizadas;
- Cinza: Simuladores Locais;
- Vermelho: Pré-requisitos para acessar nuvens e por conseguinte os computadores quânticos;
- Amarelo: Nuvens disponibilizadas pelas desenvolvedoras para acesso a seus computadores quânticos;
- Laranja: Computadores quânticos;
- Azul: Plataformas que não tem um formato definido de como irão funcionar, sendo assim promessas.

4.1 RESULTADO COMPARATIVO

De acordo com as informações disponíveis no material de apoio das plataformas estudadas, foi possível eleger uma plataforma para utilização no estudo de caso.

O pyQuil tem uma versão beta que não é disponibilizada para o público e não contém ferramentas de visualização do circuito quântico gerado. Ao tentarmos utiliza-lo nos deparamos com diversos empecilhos, principalmente relacionados a ser uma plataforma fechada e estar em beta, impossibilitando a sua utilização.

O Cirq está em nível alfa, não tem interface amigável com o usuário, com pouco material de apoio e linguagem de difícil compreensão e aprendizado. Com o correto investimento é possível que venha a se tornar um concorrente de peso, mas por hora ele não é uma plataforma viável.

O Quantum Development Kit é uma plataforma muito completa, apesar de ter uma instalação complexa para usuários inexperientes, sendo recomendado para desenvolvedores que já tenham experiências com C#. Acreditamos que ele possa vir a ter um grande espaço em um futuro próximo, mas por limitações de tempo decidimos por bem prorrogar seu estudo para trabalhos futuros.

O ProjectQ e o Qiskit se mostraram plataformas viáveis, com boa documentação e com acesso remoto aos computadores quânticos da IBM. Porém o Qiskit se mostrou mais completo que o ProjectQ com relação a ferramentas disponíveis, a exemplo das ferramentas de simulação de ruído, além de ter uma documentação mais amigavel para programadores mais inexperientes.

Considerando estes fatores é possível afirmar que o Qiskit é uma ferramenta mais desenvolvida e com uma melhor curva de aprendizado, cumprindo os requisitos para realização das simulações do estudo de caso.

5 ALGORITMOS DE CRIPTOGRAFIA QUÂNTICA ATUAIS

5.1 BB84

O primeiro protocolo de QKD (Quantum Key Distribution) foi publicado em 1984 por Charles Bennett e Gilles Brassard , recebendo a sigla BB84 como nomenclatura por causa das letras iniciais dos sobrenomes dos autores e do ano de publicação. (BENNETT, BRASSARD, 1984)

O protocolo se baseia no princípio da incerteza de Werner Heisenberg (NÚÑEZ, NEVES, 2003) (HEISENBERG, 1927) para a definição da chave secreta sem o acesso de um possível observador, além de usá-lo para a detecção deste observador.

O protocolo define um processo de comunicação por meio de um canal quântico e de um canal clássico, ambos inseguros, que tem como resultado uma chave secreta que pode ser usada posteriormente em um protocolo de criptografia clássica com chave secreta, como o DES (Data Encryption Standars) (COPPERSMITH, 1994), por exemplo. O processo tem como base as ações de um emissor que será chamado de Alice, um receptor chamado de Bob e um observador, chamado de Eve.

O protocolo define a transmissão de bits através de um canal quântico inseguro. Os bits podem ser transmitidos em duas bases de com diferentes ângulos de polarização para cada bit. A exemplo, temos uma base com o bit 0 em 0° e o bit 1 em 90° que a titulo de simplificação serão chamados de V (vertical) e H (horizontal) da base +, respectivamente. Na outra base, 0 assume o ângulo de 45° e 1 assume o ângulo de 135° chamados de D (diagonal) e A (adiagonal) da base *, respectivamente.

Na base diagonal, o qubit $|0\rangle$ é mapeado em $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e o bit $|1\rangle$ é mapeado em $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Desta forma, considerando uma escolha aleatória de bases, a Eve não pode ter conhecimento da base na qual cada bit foi polarizado. Sendo assim, os bits que forem interceptados têm um percentual de chance de serem lidos na polarização correta. Caso isto não aconteça, o qubit colapsa, com probabilidade de 50%, aleatoriamente em 1 ou em 0, gerando erros na geração da chave que denunciam a presença de um observador.

Os dados empíricos que definem as curvas probabilísticas de resposta de cada evento aleatório pertencente ao processo de distribuição de chave contido no protocolo BB84 estão contidos na Seção 6 do estudo de caso.

A definição da chave segue os seguintes passos, sem a interferência de um observador:

Alice gera um conjunto aleatório de bits que são enviados para Bob, pelo canal quântico, com polarizações randômicas:

Tabela 1 - Qubis gerados por Alice

Bit	0	0	0	1	1	0	1	1	0
Base	+	*	+	*	*	+	*	+	+
Polarização	H	D	H	A	A	H	A	V	H

Fonte: Os autores (2019)

Bob recebe os bits e efetua as medições com uma escolha randômica de bases:

Tabela 2 – Bases e medições realizadas por Bob

Base	+	*	*	+	*	*	+	+	*
Medição	0	0	1	1	1	1	1	1	1

Fonte: Os autores (2019)

Os bits cujas bases escolhidas para medição diferem das bases escolhidas por Alice, colapsam no valor absoluto 0 ou 1 com probabilidades iguais.

Alice e Bob comparam, pelo canal clássico, as bases utilizadas para polarização e para medição:

Tabela 3 - Comparação entre as bases de Alice e Bob

Base A	+	*	+	*	*	+	*	+	+
Chave A	0	0	X	X	1	X	X	1	X
Base B	+	*	*	+	*	*	+	+	*
Chave B	0	0	X	X	1	X	X	1	X

Fonte: Os autores (2019)

Nos casos em que as bases escolhidas por Alice e Bob diferem, os bits são descartados. Os bits restantes formam a chave que é igual para Alice e Bob.

Chave: 0011.

No caso de interferência da Eve, o processo se dá da seguinte maneira:

Alice gera um conjunto aleatório de bits que são enviados para Bob, pelo canal quântico, com polarizações randômicas:

Tabela 4 - Qubits gerados por Alice

Bit	0	0	0	1	1	0	1	1	0
Base	+	*	+	*	*	+	*	+	+
Polarização	H	D	H	A	A	H	A	V	H

Fonte: Os autores (2019)

Eve intercepta os dados e efetua a medição em bases aleatórias. Alice ainda não divulgou as bases de polarização, portanto Eve ainda não as conhece.

Tabela 5 - Bases e medições realizadas por Eve

Base	+	+	*	+	*	+	+	*	*
Medição	0	0	1	1	1	0	0	1	1

Fonte: Os autores (2019)

Os campos em vermelho diferem das informações de Alice. Eve polariza os bits medidos na mesma base em que mediu e os envia para Bob.

Tabela 6 - Bases e polarizações escolhidas por Eve

Bits	0	0	1	1	1	0	0	1	1
Base	+	+	*	+	*	+	+	*	*
Polarização	H	H	A	V	A	H	H	A	A

Fonte: Os autores (2019)

Bob mede os dados recebidos em bases aleatórias (Os campos em vermelho diferem das informações enviadas por Alice):

Tabela 7 - Bases e medições de Bob após Eve ter interferido

Base	+	*	*	+	*	*	+	+	*
Medição	0	0	1	1	1	1	0	0	1

Fonte: Os autores (2019)

Alice e Bob comparam as bases pelo canal clássico:

Tabela 8 - Comparações realizadas por Alice e Bob após interferência de Eve

Base a	+	*	+	*	*	+	*	+	+
Chave A	0	0	0	1	1	0	1	1	0
Base B	+	*	*	+	*	*	+	+	*
Chave B	0	0	1	1	1	0	0	0	1

Fonte: Os autores (2019)

Os bits polarizados por Alice e medidos por Bob em bases diferentes são descartados.

Alice e Bob comparam bits aleatórios da chave obtida pelo canal clássico:

Tabela 9 - Alice e Bob comparam os qubits com a base correta

Chave A	0	0	X	X	1	X	X	1	X
Chave B	0	0	X	X	1	X	X	0	X

Fonte: Os autores (2019)

A partir do número bits diferentes na fração da chave comparada é possível definir a presença ou não de um observador. Caso não seja detectado um observador, a parte divulgada da chave é descartada e o restante forma a chave definitiva. Caso contrário, a chave é descartada e o processo é feito novamente, de preferência utilizando outro canal.

É importante citar que, segundo o teorema da não clonagem, não é possível copiar bits quânticos sobrepostos com exatidão. Do contrário, a Eve poderia clonar os bits enviados pela Alice quantas vezes necessárias e medi-los aleatoriamente de forma a obter as distribuições probabilísticas do qubit e, portanto, obter o bit sobreposto. Este processo burlaria o princípio da incerteza de Heisenberg.

5.2 E91

Artur K. Ekert criou em 1991, um protocolo de QKD baseado em entrelaçamento que utiliza o estado de Bell $|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ na transmissão de chaves secretas.

O canal quântico neste protocolo emite singletos, ou seja, duas partículas emaranhadas de acordo com o estado de Bell. Alice e Bob recebem um constituinte do singleto cada um. Então Alice e Bob efetuam a medição do singleto em bases aleatórias e comparam as bases. O resultado da medição, nos casos em que a medição é feita da mesma forma, deve ser o mesmo.

Portanto, o protocolo E91 pode ser considerado uma adaptação dos princípios do protocolo BB84 para utilização de emaranhamento. (RIGOLIN, RIEZNIK, 2005)

6 RESULTADOS

Utilizando os softwares mencionados na Seção 1, realizamos simulações utilizando o protocolo BB84, variando em cada uma delas a quantidade de qubits revelados, medindo o erro provocado por esse aumento.

Para aplicação da polarização diagonal no simulador, como citado na Seção 5.1, é necessário mapear o qubit $|0\rangle$ para $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ e o qubit $|1\rangle$ para $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Esta polarização é equivalente ao resultado obtido na aplicação da porta de Hadamard.

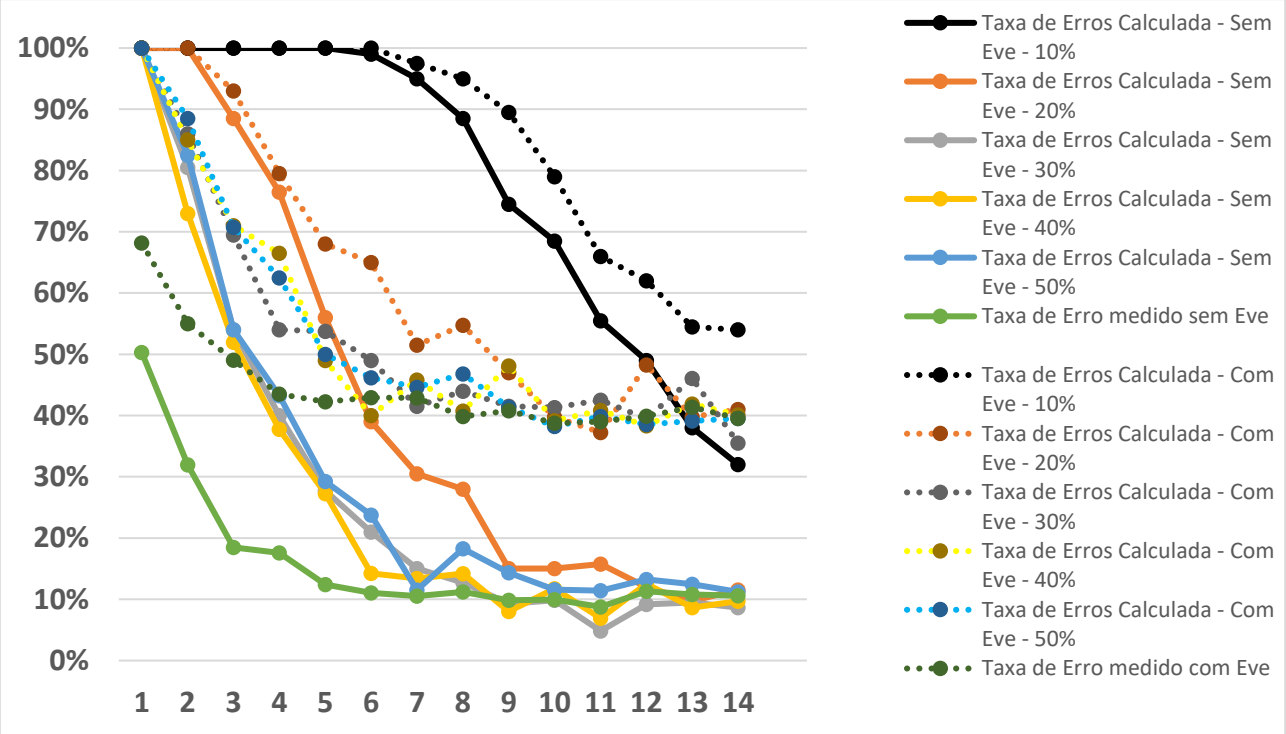
Como explanado no item 5.1 todas as portas quânticas são inversas de si mesmas, sendo assim para realizar a medição do qubit em polarização diagonal é necessária a aplicação de uma porta de Hadamard.

O processo de QKD utilizando o protocolo BB84 foi executado no QisKit. Os códigos utilizados para execução do protocolo e obtenção de resultados estatísticos encontram-se no repositório GitHub disponível em (Plácido, Fernandes, 2019).

Para verificar sua a eficiência, o protocolo BB84 foi simulado múltiplas vezes, variando a quantidade de qubits que compõem o conjunto aleatório original gerado por Alice de 1 até 14 qubits. Esse valor limite é imposto pois a simulação de erros de um computador quântico é possível apenas com os valores de tempos de depolarização e relaxação térmica de cada porta quântica do computador quântico, ou seja, a função que simula erros gerados por um computador quântico na plataforma de simulação da IBM se baseia nos computadores quânticos disponíveis. Dado que o maior computador disponibilizado pela IBM tem 14 Qubits, esse valor passa se tornar o limite superior das simulações com erro.

Os resultados de erro obtidos são mostrados na Figura 12, onde as linhas tracejadas correspondem a taxa de erros calculada com um invasor e as linhas contínuas representam as taxas de erros calculadas sem um invasor. Onde entende-se por taxa de erro calculada, a taxa de erro de uma amostra percentual, enquanto que a taxa medida considera a chave completa.

Figura 12 – Taxas de erros medidas e calculadas



Fonte: Os autores (2019)

As linhas superiores são onde foi utilizado uma taxa de amostragem menor, enquanto que as linhas mais inferiores representam taxas de amostragem maiores.

7 DISCUSSÃO

Após analisar as curvas geradas podemos tirar algumas conclusões em relação à taxa de erro gerada tanto pela intrusão quanto pelo próprio computador quântico.

Ao analisar a Figura 12 percebemos que utilizando poucos Qubits temos uma taxa de erro considerada elevada mesmo sem um invasor. Isso se deve a probabilidade de o receptor não acertar nenhuma das bases enviadas pelo emissor. O erro gerado na simulação onde isso acontece é de 100%, afetando a taxa de erro média, como é demonstrado na Figura 12 onde o erro nas simulações com poucos qubits não converge ao valor que seria esperado baseando-se na teoria.

Para 1 Qubit a probabilidade de acerto equivale a 50%, para 2 Qubits a taxa cai para 25%, seguindo a Equação:

$$P(n) = 0.5^n \tag{11}$$

Com relação ao erro gerado pelo computador quântico podemos fixa-lo entre 10% e 15% do total, como é perceptível a partir dos 9 Qubits nas curvas na Figura 12, e mais claramente nas curvas dos gráficos da Figura 12 a partir dos 5 Qubits.

Já o erro gerado pelo invasor é mais perceptível, se estabilizando entre 40% e 50% a partir dos 5 Qubits e em 9 Qubits nos gráficos gerados na Figura 12.

Percebe-se que a utilização de 10% da chave se torna inviável para a tecnologia atual, dado que a amostra máxima teria 1.4 Qubits, gerando uma separação no erro de no máximo 22%, enquanto que esse valor alcança 36% ao se utilizar uma amostra de 20%.

O tempo de execução diferente do que se imaginava não cresceu de forma exponencial, como afirma LaRose (2019), uma explicação para esse crescimento linear pode ser a quantidade de portas quânticas utilizadas, que poderia alcançar no máximo 5 por qubit, não exigindo esforço computacional excessivo do computador.

A execução do programa nos computadores quânticos da IBM por meio da nuvem se mostrou de difícil utilização considerando os tempos de espera que chegaram a 45 minutos no computador de 14 qubits.

8 CONSIDERAÇÕES FINAIS

Entende-se que atualmente a empresa que mais se aproxima de produzir um computador quântico que possa se equiparar com um computador clássico é a IBM, por ter tanto um hardware mais avançado quanto uma comunidade mais ativa, como é discutido na Seção 4. Isso se prova pela quantidade de modificações realizadas, que supera as 3000 no projeto inteiro, enquanto que o Cirq da Google tem cerca de 900, o pyQuil cerca de 800 e os programas da Microsoft e da DWave são fechados (CIRQ, 2019), (QISKIT, 2019), (RIGETTI, 2019).

Além disso a curva de aprendizado do Qiskit se mostrou mais rápida comparada aos concorrentes, dado que uma simulação pode ser executada no Qiskit no mesmo dia da instalação, o que não ocorre com as outras plataformas, como demonstrado na Seção 4.1.

Apesar do Qiskit disponibilizar computadores quânticos reais o seu acesso se mostrou demorado e inviável, dado que o tempo de fila para o computador de 14 Qubit é de cerca de 45 minutos de acordo com os fatos citados na Seção 7. Já os de 5 Qubits tomaram cerca de 2 minutos se mostrando de utilização viável.

Dentre o BB84 e o E91 percebemos que o primeiro tende a ter a execução prática mais viável, dado que o segundo se utiliza do teorema EPR, que não é tão facilmente aplicável quanto o primeiro, como discutido na Seção 5.

Para a aplicação do BB84 em projetos reais acredita-se que seja necessária a utilização de um computador quântico com pelo menos 10 Qubits, e uma taxa de amostragem para comparação de pelo menos 20%. Isso se mostrou eficaz nos ensaios apresentados na Seção 6.

Como contribuições futuras pode-se citar a utilização de mais recursos dos computadores quânticos reais disponibilizados pela IBM, que em um futuro próximo podem estar com um menor tempo de acesso, além de uma imersão mais profunda nos kits de desenvolvimento disponibilizados pela Google, Riggeti e Microsoft, que apesar de sua utilização mais complexa podem gerar tempos de respostas melhores que o Qiskit, assim como apontado por LaRose (2019).

REFERÊNCIAS

BENNETT, C. H, Brassard, G. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984(IEEE, NewYork, 1984), pp. 175–179; IBM Tech. Discl. Bull.28,3153–3163, 1985.

BLINDER, S. M. Single-Qubit Quantum Gates on a Bloch Sphere – Wolfram Demonstrations Project. Disponível em: <http://demonstrations.wolfram.com/SingleQubitQuantumGatesOnABlochSphere/> Acesso em 10 de Maio de 2019

CARDONHA, Carlos Henrique; DE CARLI SILVA, Marcel Kenji; FERNANDES, Cristina Gomes. Computação quântica: Complexidade e algoritmos. IME-USP, 2005.

CHOU, Yao-Hsin; KUO, Sy-Yen. Test data compression for any quantum Boolean circuits. In: 2009 9th IEEE Conference on Nanotechnology (IEEE-NANO). IEEE, 2009. p. 740-743.

CIRQ Developers. Cirq: A python library for NISQ circuits. Disponível em: <https://cirq.readthedocs.io/en/stable/> Acesso em: 04 de Maio de 2019

CIRQ Developers. Cirq: A python framework for creating, editing, and invoking Noisy Intermediate Scale Quantum (NISQ) circuits. Disponível em: <https://github.com/quantumlib/Cirq> Acesso em 26 de Maio de 2019.

COPPERSMITH, Don. The Data Encryption Standard (DES) and its strength against attacks. IBM journal of research and development, v. 38, n. 3, p. 243-250, 1994.

DE BROGLIE, L. The wave mechanics and the atomic structure of matter and of radiation. In: DE BROGLIE, L.; BRILLOUIN L. Selected papers on wave mechanics London: Blackie & Son, 1928. p.113-138. Publicado originalmente no Le Journal de Physique et le Radium, n. 8, p. 255, 1927.

DIRAC, P. A. M. Quantum theory of localizable dynamical systems. Physical review, v. 73, n. 9, p. 1092, 1948.

DWAVE Sys. Meet D-Wave. Disponível em: <https://www.dwavesys.com/our-company/meet-d-wave> Acesso em: 29 de novembro de 2018.

EKERT, Artur K. Quantum cryptography based on Bell's theorem. Physical review letters, v. 67, n. 6, p. 661, 1991.

FINGERBUTH, MARK. Open-Source Quantum Software Projects. Disponível em: < https://github.com/qosf/os_quantum_software > Acesso em: 27 de Abril de 2019.

HEISENBERG, W. Z. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik, v. 43, n.3-4, p.172-198, 1927.

HO, Alan. Announcing Cirq: An Open Source Framework for NISQ Algorithms. 2018. Disponível em: <https://ai.googleblog.com/2018/07/announcing-cirq-open-source-framework.html>. Acesso em: 18 Juho 2018.

INTEL. Intel Advances Quantum and a Neuromorphic Computing Research. Disponível em: <https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/#gs.9rmbbh> Acesso em: 05 de Maio de 2019

JOHANSSON, J. R.; NATION, P. D.; NORI, F. QuTiP 2: A Python framework for the dynamics of open quantum systems. Comp. Phys. Comm. v.184, p.1234, 2013

JOHANSSON, J. R.; NATION, P. D.; NORI, F. QuTiP: An open-source Python framework for the dynamics of open quantum systems. Comp. Phys. Comm. v.183, p.1760–1772, 2012

KLAUS, Schwab; MIRANDA, D. M. A quarta revolução industrial. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

LAROSE, Ryan. Overview and Comparison of Gate Level Quantum Software Plataforms. Quantum Journal, v. 3, p. 130, 2019

MILLER, David AB. Quantum mechanics for scientists and engineers. Cambridge University Press, 2008.

NÚÑEZ, I. B.; NEVES, L. S.; RAMALHO, B. L. Uma reflexão em relação ao estudo da mecânica quântica: o caso do princípio da incerteza. OEI-Revista Iberoamericana de Educación (ISSN: 1681-5653) Espanha, p. 1, 2003

PLÁCIDO, Victor; FERNANDES, Vinicius. BB84 aplicado no Qiskit. Disponível em < https://github.com/vbiral/BB84-in-Qiskit> Acesso em 19 de Maio de 2019

QISKIT. Página Principal do GitHub. Disponível em <https://github.com/Qiskit> Acesso em 27 de Maio de 2019.

RIGETTI. Página Principal do GitHub. Disponível em < https://github.com/rigetti/pyquil> Acesso em 27 de Maio de 2019.

RIGOLIN, Gustavo; RIEZNIK, Andrés Anibal. Introduçao a criptografia quântica. Revista Brasileira de Ensino de Fısica, v. 27, n. 4, p. 517-526, 2005.

SANTOS, Alan C. The IBM Quantum Computer and the IBM Quantum Experience. Revista Brasileira de Ensino de Física, v. 39, n. 1, 2017.

SMITH, Robert S.; CURTIS, Michael J.; ZENG, William J. A practical quantum instruction set architecture, 2016.

SVORE, Krysta et al. Q#: Enabling scalable quantum computing and development with a high-level dsl. In: Proceedings of the Real World Domain Specific Languages Workshop 2018. ACM, 2018. p. 7.

TEJA, Vishnu et al. Quantum cryptography: state-of-art, challenges and future perspectives. In: Proceeding of the 7th IEEE International Conference on Nanotechnology. 2007. p. 1296-1301.

VIGNATTI, André Luıs; NETTO, Francisco Summa; BITTENCOURT, Luiz Fernando. Uma introdução à computação quântica. Departamento de Informática. UFPR, 2004.

WOOTTERS, William K.; ZUREK, Wojciech H. A single quantum cannot be cloned. Nature, v. 299, n. 5886, p. 802, 1982.