UNIVERSIDADE DO VALE DO RIO DOS SINOS
UNIDADE ACADÊMICA DE GRADUAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

ARTHUR TASSINARI CABRAL

PROPOSIÇÃO DE UMA METODOLOGIA PEDAGÓGICA PARA A APRESENTAÇÃO DO ALGORITMO DE SHOR A INICIANTES

Uma Contribuição para o Progresso da Computação Quântica Sobre o Algoritmo de Criptografia RSA

São Leopoldo
2020

ARTHUR TASSINARI CABRAL

PROPOSIÇÃO DE UMA METODOLOGIA PEDAGÓGICA PARA A APRESENTAÇÃO DO ALGORITMO DE SHOR A INICIANTES

Uma Contribuição para o Progresso da Computação Quântica Sobre o Algoritmo de Criptografia RSA

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Ciência da Computação, pelo Curso de Ciência da Computação da Universidade do Vale do Rio dos Sinos (UNISINOS)

Orientador(a): Professor PhD Rodrigo da Rosa Righi

São Leopoldo
2020

PROPOSIÇÃO DE UMA METODOLOGIA PEDAGÓGICA PARA A APRESENTAÇÃO DO ALGORITMO DE SHOR A INICIANTES: Uma Contribuição para o Progresso da Computação Quântica Sobre o Algoritmo de Criptografia RSA

Arthur Tassinari Cabral[1]
Rodrigo da Rosa Righi[2]

Resumo: O Algoritmo de Shor é um importante algoritmo quântico que está presente na base de muitas pesquisas que tratam do impacto da computação quântica sobre o algoritmo de criptografia RSA. Por meio de sua utilização, e em um ambiente adequado, este algoritmo é capaz de resolver o problema da fatoração prima, pondo em risco o algoritmo RSA, que vale-se deste problema para a estruturação da chave pública. O aprendizado deste algoritmo pode promover a aproximação de estudantes a pesquisas que envolvem o progresso da computação quântica sobre o RSA. Todavia, nota-se que a maioria dos recursos disponíveis para o estudo do Algoritmo de Shor envolvem, em grande parte, a leitura de textos corridos, ou então modelos que abordem o algoritmo sob uma perspectiva bastante técnica, não apresentando um método pedagógico que vise a aproximação a ele. Dado este cenário, o presente artigo objetiva a promoção de uma metodologia pedagógica para a apresentação do Algoritmo de Shor a iniciantes. A metodologia utilizada é uma plataforma web, que apresenta um passo-a-passo educativo, com exercícios de fixação, proporcionando a interatividade do usuário com a aplicação. Verificou-se que a plataforma foi eficiente e eficaz em apresentar o Algoritmo de Shor a iniciantes, mas que pode-se melhorar a abordagem sobre alguns dos passos do algoritmo. O artigo favorece as pesquisas que tratam do avanço da computação quântica sobre o RSA porque é capaz de aproximar a academia e pessoas da área da computação a elas, e desta forma, conseguintemente, beneficia-se a ciência da computação.

Palavras-chave: Computação Quântica. RSA. Algoritmo de Shor. Modelo Educativo. Plataforma Web

Abstract: The Shor's Algorithm is an important quantum algorithm that is present in the basis of many researches that deal with the impact of quantum computing on the RSA encryption algorithm. Through its use, and in an appropriate environment, this algorithm is able to solve the problem of prime factorization, putting the RSA algorithm at risk, which uses this problem to structure the public key. The learning about this algorithm can bring students closer to research involving the progress of quantum computing over RSA. However, it is noted that most of the resources available for the study of the Shor's Algorithm involve, mainly, the reading of body texts, or models that approach the algorithm from a very technical perspective, without presenting a pedagogical method that proposes a better access to it. Given this scenario, the present article aims to promote a pedagogical methodology for the presentation of the Shor's Algorithm to beginners. The methodology used is a web platform, which presents an educational step-by-step, with fixation exercises, providing user interactivity with the application. It was found that the platform was efficient and effective in introducing the Shor's Algorithm to beginners, but that one can improve the approach on some of the steps of the algorithm. The article favors research that deals with the advancement of quantum computing over RSA because it is able to

[1]Graduando em Ciência da Computação pela Unisinos. Email: arthurtcabral@gmail.com
[2]Doutor em Ciência da Computação. Coordenador do PPG em Computação. Email: rrrighi@unisinos.br

bring academia and people from the area of computing closer to them, and thus, consequently, benefits computer science.

Keywords: Quantum Computing. RSA. Shor's Algorithm. Educational Model. Web Platform

1 INTRODUÇÃO

O Algoritmo de Criptografia RSA - presente em muitas aplicações, como e-mails, certificados digitais e serviços de nuvem como a Google G Suite (NISHA; FARIK, 2017) - tem a sua segurança baseada, entre outras operações, na fatoração prima, valendo-se da dificuldade que os computadores clássicos têm em processar esta operação. Há de se dizer que, dentro do paradigma da computação clássica, um computador levaria muito tempo para o término do processamento da fatoração prima, pois esta operação matemática é extremamente exigente em recursos computacionais (MAVROEIDIS et al., 2018). Mesmo assim, a computação clássica tem alcançado êxitos neste sentido, de fatorar grandes números. Fato é que algumas versões do RSA, como por exemplo o RSA-768, já foi fatorado (KLEINJUNG et al., 2010), dada a utlização de um alto poder computacional.

No entanto, com a ascenção da computação quântica, o problema da fatoração prima pode ser mais facilmente resolvido. Levando-se em consideração que o Algoritmo RSA utiliza este problema para a criptografia da chave pública, chega-se a hipótese de que o algoritmo pode, futuramente, vir a estar com a sua segurança comprometida. Esta hipótese é reiterada levando em consideração que a ciência da computação, principalmente no decorrer da última década, vem apresentando uma série de trabalhos sobre o tema que mostram resultados promissores no que se refere ao processamento da operação matemática de fatoração prima dentro do paradigma da computação quântica.

O avanço da computação quântica sobre o Algoritmo de Criptografia RSA pode ser notado a partir da verificação da seguinte linha do tempo: Em 2013, por exemplo, foi proposta a ideia de um circuito para a fatoração dos números 51 e 85 utilizando 8 *qubits* (GELLER; ZHOU, 2013), por meio da utilização do Algoritmo de Shor - algoritmo quântico para fatoração prima. Mais tarde, com o uso de uma técnica que utiliza ressonância magnética nuclear, a metodologia Minimization, foi possível a fatoração do número 56153, contando com 4 *qubits* (DATTANI; BRYANS, 2014). Em 2018, por meio do recozimento quântico, foi realizada a fatoração prima do número 376289, utilizando 94 *qubits* (JIANG et al., 2018). No mês de junho de 2019, uma metodologia apresentada em uma pesquisa efetuada na China, valendo-se do recozimento quântico, foi capaz de fatorar o número 1005973 (PENG et al., 2019).

Apesar dos resultados promissores que a computação quântica apresenta, referentes a sua ação sobre o Algoritmo de Criptografia RSA, é importante destacar que esta categoria da computação ainda está distante de efetuar a quebra do algoritmo: O RSA, em versões mais atuais, utiliza números de, por exemplo, 2048 bits em sua chave pública, e as técnicas quânticas mostradas por pesquisas realizadas ao longo dos últimos 10 anos foram capazes de fatorar números

bastante menores, de acordo com os dados exibidos anteriormente. Dentre estes números, o de maior tamanho é de 20 bits, o que dista muito do que está sendo usado pelo Algoritmo RSA na época presente.

A continuação do progresso da computação quântica sobre o Algoritmo de Criptografia RSA seria de grande contribuição para a segurança de aplicações, visto que, conforme estuda-se as fraquezas deste algoritmo pelo avanço da referida categoria da computação, cresce a necessidade do estudo sobre criptografia pós-quântica, que é uma categoria de criptografia que comporta os algoritmos que não são vulneráveis a ataques quânticos (WOLF, 2019). Além disto, o estudo relacionado a tal progresso está associado ao estudo sobre melhorias de hardware das máquinas quânticas. Cabe dizer que estas máquinas, atualmente, apresentam a alta necessidade de lidarem com ruídos de ambiente que podem incidir sobre o funcionamento delas (RESCH; KARPUZCU, 2019). Desta forma, este progresso beneficia a ciência, enriquecendo as áreas de segurança de aplicações, estratégia de segurança da informação e arquitetura de computadores.

No contexto do avanço da computação quântica sobre o RSA, há o Algoritmo de Shor, que é um algoritmo quântico para a fatoração de números inteiros (WOLF, 2019). Este algoritmo, se executado em um computador quântico universal - computador projetado para operar qualquer tarefa (MAVROEIDIS et al., 2018), e não apenas uma em específico - tolerante a ruídos, pode ser capaz de quebrar o Algoritmo RSA (MENGONI et al., 2020). Ainda conforme Mengoni et al. (2020), nos últimos anos, foram propostas várias implementações baseadas no Algoritmo de Shor, mas visando a execução em recozedores quânticos - máquinas quânticas projetadas para problemas de otimização combinatória (ONODERA et al., 2019). Dada a presença do Algoritmo de Shor em pesquisas referentes ao progresso da computação quântica sobre o RSA, pode-se afirmar que um dos modos de contribuir para com elas é pelo ensino do algoritmo.

Todavia, atualmente, nota-se uma escassez de ferramentas que objetivem o ensino do Algoritmo de Shor a iniciantes, valendo-se de uma abordagem pedagógica para este propósito. As ferramentas utilizam muitos termos técnicos, ou usam apenas texto, o que pode dificultar a aprendizagem sobre o algoritmo. Por exemplo, em "Implementation of Shor's Quantum Factoring Algorithm using ProjectQ Framework"(WICAKSONO; WICAKSANA, 2019), embora seja abordado o uso de um simulador quântico para executar o Algoritmo de Shor, propiciando a aproximação de estudantes ao tema, este trabalho não se propõe ao ensino do algoritmo a principiantes. Outro exemplo é a implementação deste algoritmo presente no repositório da Microsoft (MICROSOFT, 2020): Ela não o explica visando o iniciante no assunto, e este aprendizado, neste caso, valeria-se da interpretação do código e dos comentários nele escritos.

Neste sentido, o presente artigo tem como objetivo a promoção de uma metodologia pedagógica para apresentar o Algoritmo de Shor a iniciantes. Com esta apresentação, mais pessoas estarão cientes sobre um algoritmo atualmente compreendido por pesquisas que tratam da análise de impacto da computação quântica sobre o RSA, aproximando tais pesquisas aos usuários, e assim, possibilitando a contribuição para o progresso destes trabalhos, visando os benefícios que eles podem trazer à ciência. A metodologia pedagógica consiste em uma plataforma web

que conta com uma sequência de passos amigáveis para o seu propósito, constituindo-se de dois módulos de estudo, sendo o primeiro responsável por fazer uma introdução à computação quântica e o segundo por abordar o algoritmo. O formato destes módulos é em lâminas, tratando de apresentar a teoria e propor exercícios na forma de perguntas de múltipla escolha.

Este trabalho também busca viabilizar a aproximação de estudantes acadêmicos e graduados, relacionados a algum curso da área da informática, à própria computação quântica. Conforme Pamplona (2018), os resultados dela "*podem envolver e inovar outros campos de estudo do meio científico*", tais como "*a Matemática computacional, Química quântica, Física quântica, Ciência da Computação, dentre outros*". As referidas zonas de estudo que seriam inovadas com o avanço da computação quântica compõem um fator que motiva a elaboração de um trabalho que visa o aumento deste fortalecimento, por meio da ampliação da proximidade entre a academia e diplomados, e ela.

O artigo está estruturado em seis seções: Feita esta introdução, é apresentada a fundamentação teórica, relacionada ao Algoritmo de Criptografia RSA e à computação quântica, contemplando o Algoritmo de Shor. Na sequência, são apresentados os trabalhos relacionados ao tema do artigo. Na seção seguinte, apresenta-se o modelo proposto pela presente pesquisa, comportando a metodologia pedagógica para o ensino do Algoritmo de Shor para iniciantes e o método de avaliação dela. Após isto, mostra-se uma seção que trata dos resultados da avaliação. Por fim, é apresentada a seção de considerações finais e trabalhos futuros, que conclui o presente artigo.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção compreende uma série de conceitos que visam o entendimento de elementos relacionados ao que é proposto no presente trabalho. Inicia-se esta seção com a conceituação do Algoritmo de Criptografia RSA, tratando de englobar o problema da fatoração prima, utilizado pelo algoritmo, além de abarcar a quebra do RSA-768 bits pela computação clássica. Na sequência, apresenta-se uma subseção dedicada à computação quântica. Tal subseção explica o que é a computação quântica, envolvendo outras subseções nela presentes, tendo como temas o Qubit, a Sobreposição, o Entrelaçamento, o Algoritmo de Shor e o Computador Quântico Universal.

2.1 O Algoritmo de Criptografia RSA e a Utilização do Problema da Fatoração Prima

Em 1978, os cientistas Ronald Rivest, Adi Shamir e Leonard Adleman lançaram o Algoritmo de Criptografia RSA, defendendo a ideia de que, como a "Era do Correio Eletrônico"se aproximava, duas propriedades do modelo de "correio em papel"deveriam ser mantidas: A privacidade e a assinatura das mensagens. Com estas propriedades evidenciadas, os cientistas propuseram um algoritmo que abarcasse, nas palavras deles, "o elegante conceito"de criptosis-

tema de chave pública, inventado, em 1975, por Diffie e Hellman. Este algoritmo é o RSA, que tem a sua segurança baseada na dificuldade em efetuar a fatoração prima de grandes números inteiros.

O RSA, a seu favor, faz uso de alguns teoremas matemáticos para a composição do cálculo das chaves de criptografia e descriptografia, de modo que um interceptador, tendo somente a posse de tais chaves públicas, não consiga efetuar a quebra da criptografia da mensagem. Dentre os teoremas utilizados, citam-se a fatoração prima de Euclides, o problema do logaritmo discreto, a função totiente de Euler e o teorema de Euler (MAVROEIDIS et al., 2018). A publicação do algoritmo, em 1978, defendia a ideia de que o número público formado pela multiplicação de dois números primos precisa ter, para a segurança operacional do RSA, pelo menos 200 dígitos. Na época, o algoritmo mais veloz para a fatoração prima era capaz de fatorar um número de 50 dígitos em 3,9 horas, e um de 200 dígitos em $3,8 \times 10^{25}$ anos.

Mesmo ao longo dos anos 2010 até a atualidade, a fatoração prima de um grande número inteiro ainda é uma atividade custosa para a computação clássica. Em 2010, a ciência foi capaz de quebrar o RSA-768, uma versão do Algoritmo RSA que tem a sua chave com o tamanho de 768 bits (KLEINJUNG et al., 2010). Dentre as características de arquitetura utilizadas para este feito, cita-se um cluster de 56 nodos de 2.2GHz dual hex-core AMD, e também uma variedade de clusters ALADDIN-G5K. Estima-se que, se fosse considerado um single core 2.2GHz da AMD, seria preciso cerca de 2 mil anos de computação para executar todo o processamento necessário.

2.2 Computação Quântica

A computação quântica é um ramo científico da computação que utiliza de conhecimentos da física quântica, referentes mais especificamente à mecânica quântica, para a operabilidade, elaboração teórica, e a funcionalidade dos computadores quânticos. Ao passo que a mecânica quântica relaciona-se ao estudo dos fenômenos que ocorrem em micropartículas físicas (MAVROEIDIS et al., 2018) – partículas subatômicas – a computação quântica efetua uso do tema de estudo da mecânica quântica a seu favor, empregando o conceito e a aplicação de fenômenos como a sobreposição (superposition) e o entrelaçamento (entanglement). Estes fenômenos são aplicados sobre os bits quânticos, também denominados qubits.

2.2.1 Bit Quântico – Qubit

O bit quântico, também conhecido por qubit, é o bit da computação quântica. Na computação clássica, o bit clássico é determinístico ao passo em que opera, necessariamente, sobre um entre os dois seguintes valores: 0 e 1. Já na computação quântica, em contraste ao determinismo da computação clássica, os qubits tem a capacidade de assumir 3 estados: 0, 1 e um estado formado por 0 e 1 juntos, sendo 0 + 1 (BARRENO, 2002). Sendo assim, dois qubits

podem representar, em uma unidade de tempo, os valores 00, 01, 10 e 11 (KIRSCH, 2015). Pode-se dizer que o qubit, dado a sua característica de poder apresentar o estado 0 + 1, é um objeto contínuo (DYAKONOV, 2019).

2.2.1.1 Sobreposição (Superposition)

A sobreposição é um evento que define o qubit quando ele está no estado |0 + 1). Uma analogia para tal evento é o experimento mental do gato de Schrödinger, proposto pelo físico austríaco Erwin Schrödinger - laureado com o Nobel de Física em 1933 graças à equação denominada "Equação de Schrödinger", que consiste em obter soluções capazes de fornecer informações fundamentais sobre o comportamento de uma partícula-onda (ATTUX et al., 2012): Imagina-se um gato em uma caixa fechada, junto a um frasco de vidro contendo um líquido radioativo, e enquanto a caixa estiver fechada, o gato não está vivo ou morto, mas em um estado formado pela união dos dois estados, denominado "vivomorto". Este estado é mantido até que faça-se a sua medição pela abertura da caixa, forçando a natureza a responder sobre o estado do gato. Pode-se entender o qubit em sobreposição, no estado |0 + 1), como sendo o gato na caixa.

2.2.1.2 Entrelaçamento (Entanglement)

O entrelaçamento é um evento que ocorre quando dois qubits têm e mantém uma ligação robusta entre eles a ponto de não ser possível descrever o qubit A sem que o qubit B também seja descrito. Desta forma, se um dos qubits entrelaçados tiver seu valor alterado, o outro também terá, independentemente da distância entre eles (MAVROEIDIS et al., 2018). Conforme o número de qubits entrelaçados aumenta, o número de valores que podem ser processados em apenas uma operação aumenta também. Uma aplicação de destaque do entrelaçamento quântico é o teletransporte, que permite a transmissão de um estado quântico entre qubits de maneira instantânea, não havendo transmissão de materia, mas sim de informação (BONILLO, 2013).

2.2.2 Algoritmo de Shor

Em 1994, Peter Shor, matemático estadunidense, desenvolveu um algoritmo que tinha como objetivo a fatoração prima de um número N com o comprimento de L bits. Diferentemente de metodologias clássicas até então conhecidas, este algoritmo tinha a peculiaridade de ser um algoritmo quântico, e graças a isso, bem como à forma de sua implementação, a expectativa era a de efetuar a fatoração prima em um tempo bastante menor em relação a tais metodologias. A publicação de tal algoritmo levou a afirmações generalizadas de que computadores quânticos iriam aniquilar a criptografia clássica, ou ao menos as de chave pública (BERNSTEIN et al., 2017). Dizia-se, também, que “Quando os primeiros serviços quânticos forem construídos, a segurança de sistemas de chave pública criptografada simplesmente desaparecerá”.

Shor (1996), no artigo "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", conta que seu trabalho mostra que problemas como o da fatoração prima, utilizado pelo algoritmo RSA, podem ser resolvidos por um computador quântico em tempo polinomial, considerando uma pequena probabilidade de erro. Além disso, o autor relata que se por acaso o único uso da computação quântica fosse a atuação sobre logarítmos discretos e fatoração prima, então trataria-se de uma técnica cujo objetivo é impedir o funcionamento de algoritmos de criptografia de chave pública, evidenciando a ação que a computação quântica pode efetuar sobre estes algoritmos. Em adição, a cientista Anastasia Marchenkova [3] (2020), em entrevista online, mencionou que o Algoritmo de Shor é "o padrão para a quebra do RSA".

Ainda que o Algoritmo de Shor possa ser uma boa implementação no que se refere à fatoração prima, é importante mencionar que, segundo Gidney e Ekerå (2019), os computadores quânticos atuais ainda estão longe de serem capazes de executar este algoritmo levando em consideração números de tamanhos relevantes, utilizados por algoritmos de criptografia. Isto ocorre por conta do ruído presente nos computadores quânticos universais, que pode tornar a execução da aritmética em um computador quântico mais custosa do que em um computador clássico. Contudo, caso este ruído seja melhor tratado, o Algoritmo de Shor pode ser eficaz para fatorar grandes números inteiros. No Algoritmo 1, que consta na página a seguir, é apresentado um passo-a-passo da execução do Algoritmo de Shor. Este passo-a-passo foi escrito seguindo as instruções presentes em "Princípios Fundamentales de Computación Cuántica"(BONILLO, 2013).

2.2.3 Computador Quântico Universal

Um computador quântico universal é um computador quântico desenvolvido para operar qualquer tarefa (MAVROEIDIS et al., 2018), não sendo, portanto, para um único propósito, como aprendizado de máquina ou otimização de problemas NP-Completo. É possível efetuar a implementação de tais computadores com uma variedade de tecnologias físicas, como, por exemplo, fótons ou supercondutores (RESCH; KARPUZCU, 2019). Estes computadores não existem em abundâcia porque são bastante sensíveis a ruídos, e sendo assim, pode-se dizer que são de difícil construção. As condições de ambiente necessárias, difíceis de serem criadas, envolvem a temperatura próxima ao zero absoluto e proteção contra radiação (RESCH; KARPUZCU, 2019).

3 TRABALHOS RELACIONADOS

Os trabalhos relacionados aqui apresentados foram selecionados com base em pesquisas efetuadas na Plataforma Arxiv, no Google Acadêmico e no indexador de pesquisas Google. Es-

[3] Pesquisadora na Bleximo Corporation. Especialista em Física Atômica, Molecular e Ótica.

Algoritmo 1: Algoritmo de Shor

Entrada: Um número N a ser fatorado e um número pseudoaleatório c para um fator de N.

Saída: Os fatores de N.

início

Calcular o MDC(c, N);

if MDC(c, N) $\neq$ **1 then**

Dividir N pelo valor do MDC(c, N);

Finalizar execução do algoritmo.

else

repita

`Agora, precisa-se encontrar o período r da função f(x) =` c^x `mod N.`

Iniciar um registrador quântico de entrada no estado 0, com log2N qubits;

Iniciar um registrador quântico de saída no estado 0, com log2N qubits;

Constituir a função f(x) apresentada como uma função quântica;

Aplicar a função f(x) no estado |0) quântico;

`O melhor candidato ao período r é o menor valor possível para r.`

repita

Aplicar a Transformada Quântica de Fourier no registro de entrada;

Medir o resultado, que vai apresentar um valor y;

Converter y/N em uma fração irredutível, gerando um possível valor para r;

até Localizar o melhor candidato ao periodo r, dentre os presentes na sobreposição quântica;

if Os fatores de N são o MDC(a$^{r/2} \pm$ **1, N) then**

Finalizar execução do algoritmo

até Encontrar os fatores de N;

end

fim

tas pesquisas foram feitas no mês de agosto de 2020, utilizando os seguintes textos de busca: "Learning Shor's Algorithm", "Shor's Algorithm Implementation for Students", "Learn Shor's Algorithm", "Aprendendo o Algoritmo de Shor"e "Shor's Algorithm Explained student platform". Dentre as fontes localizadas, selecionou-se as apresentadas pela tabela 1 devido à proximidade, dados alguns fatores relacionados a seus respectivos conteúdos, à ideia da presente

pesquisa. Levou-se em consideração trabalhos que, dadas as suas próprias características, pudessem proporcionar a aproximação entre estudantes iniciantes e o Algoritmo de Shor.

O progresso da computação quântica sobre o algoritmo de criptografia RSA é visto, em grande parte, nos trabalhos científicos que lidam com a resolução do problema da fatoração prima, uma vez que, conforme consta na subseção 2.1, o RSA tem a sua segurança muito baseada neste problema. O Algoritmo de Shor é um grande candidato a efetuar a quebra do RSA, dada a sua capacidade de resolver o problema mencionado. Destaca-se que, atualmente, este algoritmo quântico está presente na base de muitas pesquisas relacionadas a tal tema, o que reforça a importância do estudo de tal algoritmo. Entretanto, quando recorre-se a pesquisa por métodos de ensino do algoritmo, visando iniciantes no assunto, nota-se uma escassez de metodologias pedagógicas neste sentido. Visto isto, os trabalhos apresentados pela presente seção estão relacionados a esta ideia, que está vinculada ao objetivo deste artigo.

Os autores de "Implementation of Shor's Quantum Factoring Algorithm using ProjectQ Framework"(WICAKSONO; WICAKSANA, 2019), comunicam a utilização da linguagem de programação Python e de um simulador quântico da ProjectQ para a implementação do Algoritmo de Shor. No corpo do artigo, é apresentado um passo-a-passo do funcionamento do algoritmo, mas que é sucinto, detalhando brevemente as etapas do processo, não indo ao encontro da proposta do presente trabalho. Dado isto, mesmo com o uso de um simulador quântico - o que pode aproximar o tema de estudantes iniciantes - não há a abordagem do Algoritmo de Shor de maneira pedagógica por parte desta fonte.

A Microsoft possui um repositório no GitHub denominado "Quantum", com uma série de exemplos de códigos escritos em Q#, linguagem de programação presente no QDK - Quantum Development Kit - para, entre outros propósitos, o desenvolvimento de programas relacionados ao paradigma quântico da computação, que podem ser testados com o simulador disponibilizado pelo kit (MICROSOFT, 2020). Dentre os exemplos que constam no repositório, há o Algoritmo de Shor, porém, ele não apresenta um detalhamento didático de acordo com o desejado pelo presente artigo, uma vez que o aprendizado sobre o algoritmo, neste caso, valeria-se da interpretação do código e da leitura dos comentários nele escritos.

As fontes Qiskit 0.20.0 Documentation - da IBM; Shor's Algorithm with Code - da plataforma Quantum Computing UK; e Shor's Algorithm in Quantum Computing - da plataforma Top Coder, são fontes de ensino sobre o Algoritmo de Shor que efetuam um detalhamento a respeito do algoritmo de forma mais didática, tratando de seu passo-a-passo com explicações neste sentido. No entanto, as referidas fontes valem-se, em suma, da utilização de texto corrido e exemplos. Estas fontes não promovem exercícios que possibilitem ao estudante iniciante o acompanhamento do progresso de seu aprendizado ao longo do estudo. Portanto, tais ferramentas não vão totalmente ao encontro do objetivo do presente artigo.

Apresenta-se a tabela 1, que conta com 5 colunas. A primeira coluna, denominada "Trabalhos", apresenta a fonte inclusa na tabela. A coluna "Dedicação Exclusiva"mostra se a fonte em questão aborda o Algoritmo de Shor de forma exclusiva, isto é, com foco somente na apresen-

tação deste algoritmo. Em "Ensino Teórico", visa-se exibir se a fonte aborda a teoria do Algoritmo de Shor no sentido de ensiná-la ao iniciante. A coluna "Exemplos de Utilização"indica se a fonte em questão apresenta exemplos de uso do Algoritmo de Shor, visando detalhar as suas instruções. Por fim, a coluna "Exercícios Interativos"mostra se a fonte disponibiliza exercícios interativos para o acompanhamento do processo de aprendizagem.

Tabela 1 – Comparativo Entre Os Trabalhos Relacionados

Trabalhos	**Dedicação Exclusiva**	**Ensino Teórico**	**Exemplos de Utilização**	**Exercícios Interativos**
Implementation of Shor's Quantum Factoring Algorithm using ProjectQ Framework	Não	Não	Não	Não
Microsoft Quantum Repository	Não	Não	Sim	Não
Shor - Qiskit 0.20.0 Documentation	Sim	Sim	Sim	Não
Quantum Computing UK - Shor's Algorithm with Code	Sim	Sim	Sim	Não
Top Coder - Shor's Algorithm in Quantum Computing	Sim	Sim	Sim	Não
Hello Shor!	**Sim**	**Sim**	**Sim**	**Sim**

Tendo em vista os trabalhos relacionados analisados na presente seção, nota-se que há uma escassez de ferramentas pedagógicas que visem o ensino do Algoritmo de Shor para estudantes iniciantes. Constata-se tal escassez quando percebe-se que, atualmente, as pesquisas tratam o Algoritmo de Shor já em sua aplicação final, ou então o ensinam por meio de abordagens que valem-se apenas de leitura e interpretação de texto. As ferramentas atuais não disponibilizam exercícios interativos, que visam efetuar um acompanhamento no processo de aprendizagem do estudante. Desta forma, por mais que estas ferramentas efetuem o ensino do Algoritmo de Shor, esta ação pode ser aprimorada, dado a maneira como elas se apresentam.

4 HELLO SHOR!

Esta seção apresenta o modelo que o presente trabalho propõe para, juntamente com a pesquisa até aqui elaborada, alcançar o objetivo proposto. Cabe lembrar que o objetivo do presente trabalho é promover uma metodologia pedagógica para o ensino do Algoritmo de Shor a iniciantes, visto que, com este ensino, mais pessoas estarão cientes sobre um algoritmo atualmente utilizado em pesquisas que tratam da análise de impacto da computação quântica sobre o RSA,

podendo colaborar para o progresso destas pesquisas. A Plataforma Hello Shor! se caracteriza como sendo uma ferramenta que atua como ponto de partida para o estudo do tema das pesquisas mencionadas.

4.1 Decisões de Projeto

O modelo proposto consiste na promoção de uma plataforma educativa denominada Hello Shor!, que tem como objetivo a apresentação do Algoritmo de Shor a iniciantes, que é um conhecido algoritmo que utiliza a computação quântica para a fatoração de números inteiros. De maneira mais específica, a plataforma tem o intuito de efetuar uma introdução ao referido algoritmo, viabilizando uma metodologia pedagógica em formato de lâminas, dispondo de conteúdo teórico e da prática de exercícios. Destaca-se que a metodologia pedagógica da Hello Shor!, orientada a iniciantes no tema, valendo-se da utilização de exercícios interativos, é a principal característica dela, diferenciando-a dos trabalhos relacionados apontados na tabela 1, mostrada na seção 3 do presente artigo.

A Hello Shor! tem como público-alvo acadêmicos de cursos da área da computação, como por exemplo, ciência da computação, análise e desenvolvimento de sistemas e sistemas de informação, visando a colaboração para com o tema do impacto da computação quântica sobre o RSA. Há de se dizer que deseja-se, com o site, que os acadêmicos, desde a graduação, já estejam inteirados sobre o tema, e sendo assim, estaria-se colaborando para o seu andamento. Outro motivo para que o público-alvo seja o mencionado é o fato da plataforma considerar que os usuários já possuem conhecimentos prévios sobre a área da computação, e visto isto, ela alia este fato com a metodologia de ensino defendida por Paulo Freire (1992), que considera os conhecimentos prévios que o estudante já tem consigo:

> "É preciso que o educador saiba que o seu “aqui” e o seu “agora” são quase sempre o “lá” do educando. Mesmo que o sonho do educador seja não somente tornar o seu “aqui agora”, o seu saber, acessível ao educando, mas ir mais além de seu “aqui agora” com ele ou compreender, feliz, que o seu educando ultrapasse o seu “aqui”, para que esse sonho se realize tem que partir do “aqui” do educando e não do seu."(FREIRE, 1992)

A metodologia do presente trabalho considera, além do aspecto da obra de Paulo Freire (1992) mencionado anteriormente, alguns pontos da Teoria de Aprendizagem Significativa de David Ausubel, segundo Agra, Formiga, Oliveira, Costa, Fernandes e Nóbrega (2017). Considera-se a interação entre conhecimentos já existentes e conhecimentos que o estudante vai passar a ter, ao longo da prática com a plataforma, como parte da estratégia de ensino, uma vez que tem-se em vista que o usuário possui conhecimentos prévios a respeito da área da computação. No artigo "Análise do conceito de Aprendizagem Significativa à luz da Teoria de Ausubel"(AGRA et al.; 2017), menciona-se o significado da teoria indicada:

> "[...] uma Aprendizagem Significativa, de acordo com David Ausubel, autor da Teoria da Aprendizagem Significativa – TAS, trata-se de uma estratégia promissora em situação formal de ensino, a qual consiste na interação não arbitrária e não literal de novos conhecimentos com conhecimentos prévios (subsunçores) relevantes. Assim, a partir de sucessivas interações, um determinado subsunçor, progressivamente, adquire novos significados, torna-se mais rico, mais refinado, mais diferenciado e é capaz de servir de âncora para novas aprendizagens significativas."(AGRA et al.; 2017)

O motivo da escolha por efetuar a apresentação do Algoritmo de Shor pela plataforma proposta se deve ao fato da presença deste nas bases de pesquisas atuais que tratam do avanço do impacto da computação quântica sobre o algoritmo de criptografia RSA. Desta maneira, oportuniza-se que os estudantes tenham contato com um algoritmo presente em trabalhos recentes a respeito do assunto. Além disto, a estabelecida escolha pelo Algoritmo de Shor também sucede-se em razão de que ele é um dos principais candidatos a ocasionar o rompimento da segurança promovida pelo RSA, em concordância com o que consta na seção de introdução a este artigo.

4.2 Funcionamento

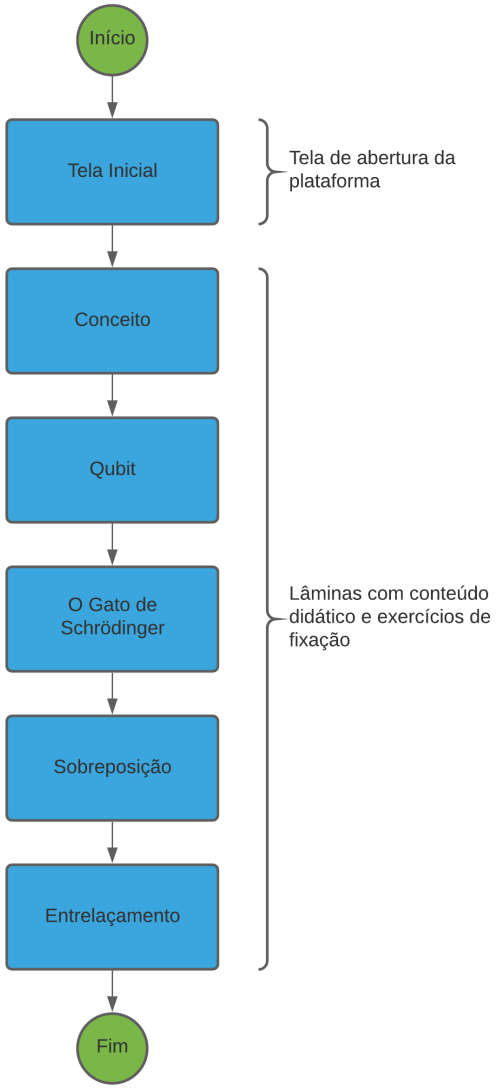
A plataforma Hello Shor! apresenta, primeiramente, uma tela inicial, e por meio dela, pode-se acessar o método educativo. A metodologia consiste na promoção de dois blocos de estudos, contemplando conteúdo teórico e perguntas de múltipla escolha em cada bloco. É importante mencionar que ambos os blocos de estudo realizam uma abordagem pedagógica, com o intuito de efetuar uma iniciação aos conteúdos. O primeiro bloco de estudos trata de conceitos relacionados à computação quântica, ao passo em que o segundo bloco promove a apresentação do estudante ao Algoritmo de Shor, falando sobre, por exemplo, seu conceito, seu objetivo e seu passo-a-passo de execução.

Conforme mencionado, o início das atividades com a Hello Shor é pela tela inicial, onde o usuário tem a possibilidade de iniciar a prática do método educativo, clicando no botão "Iniciar", e de ver mais detalhes sobre o site, por meio do clique no botão "Sobre". Ao clicar no botão "Iniciar", o site imediatamente inicia a aplicação do método educativo. A tela inicial da plataforma apresenta o logotipo da Hello Shor!, que consiste em um átomo cinza ao fundo com o nome dela sobreposto "Hello Shor!", conforme apresenta a figura 2. A escolha pela figura do átomo faz alusão à física quântica, que lida com os fenômenos que acontecem em partículas subatômicas. A coloração em azul das letras foi escolhida devido ao seu significado de confiança (WATSON, 2015).

O primeiro bloco de estudos tem o objetivo de efetuar a ambientação do usuário à computação quântica, sendo abordados conteúdos iniciais referentes a ela, tais como o conceito de computação quântica, conceituação de qubit, definição de sobreposição quântica e entrelaçamento quântico, entre outros. Este bloco inicia após o clique no botão "Iniciar"da tela inicial e

vai até o módulo sobre entrelaçamento quântico, o último antes de iniciar o segundo bloco de estudos. Estes conteúdos são apresentados no formato de lâminas, e em meio a elas, são feitas perguntas de múltipla escolha ao usuário, de maneira a promover a interatividade dele com a plataforma Hello Shor!, bem como de modo a retomar os conteúdos mostrados no decorrer das lâminas, com o intuito de garantir a excelência na qualidade do ensino. A figura 1 apresenta o fluxograma de funcionamento do primeiro bloco de estudos, que começa após a tela inicial.

Figura 1 – Tela Inicial e Primeiro Bloco de Estudos da Hello Shor!



Fonte: Autoral

O motivo dos módulos do bloco 1 seguirem a ordenação apresentada na figura 1 diz respeito à aplicação da prática pedagógica que a plataforma utiliza. Inicia-se com conceitos mais simples, de modo a introduzir o estudante à computação quântica, até alcançar o bloco 2, que lida com o Algoritmo de Shor. Os conceitos apresentados são importantes para o entendimento do funcionamento do referido algoritmo, além de serem fundamentais para a ambientação do estudante na mencionada categoria da computação. Começa-se com a conceituação de compu-

tação quântica, seguida do conceito de sua menor unidade de informação, que é o qubit. Então, abordam-se conceitos que tratam de importantes operações efetuadas com qubits: Sobreposição - Com um módulo sobre o experimento mental do Gato de Schrödinger, que explica a ideia de tal operação - e Entrelaçamento.

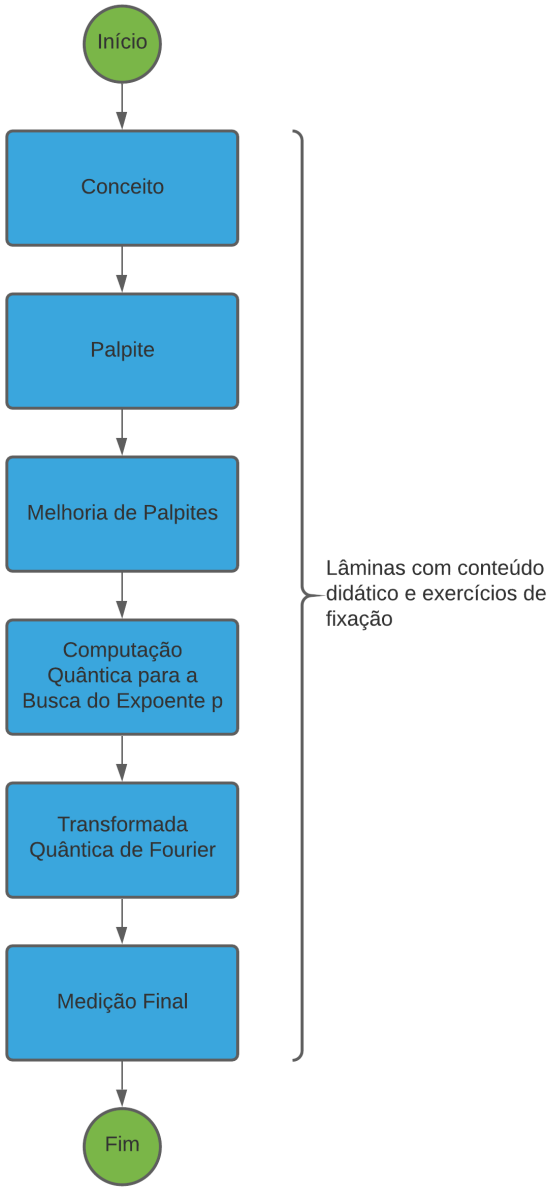
Dada a conclusão do bloco de estudos que introduz o usuário à computação quântica, inicia-se o segundo bloco, que tem o objetivo de apresentar a ele o Algoritmo de Shor, e para este processo, aborda-se o conceito, a história e o funcionamento do algoritmo. Destaca-se que este bloco também apresenta os conteúdos no formato de slides, bem como promove perguntas de múltipla escolha no decorrer deles, permitindo que o usuário fortaleça o aprendizado sobre o tema de estudo. O bloco conta com um exemplo que estabelece um cenário onde o usuário tem um cofre com moedas de ouro lacrado com o número 314191, e para abri-lo, necessita saber os fatores deste número, e para isto, precisa conhecer o Algoritmo de Shor, e assim inicia-se a apresentação do algoritmo. Ao final do bloco, o usuário conhece os fatores do número 314191, sendo possível, no cenário proposto, abrir o cofre e acessar às moedas de ouro.

A apresentação do passo-a-passo do Algoritmo de Shor foi elaborada fundamentando-se em suas próprias etapas, levando em consideração os artigos "Algoritmo de Shor e sua aplicação à fatoração de números inteiros"(FREITAS, 2010) e "Principios Fundamentales de Computación Cuántica"(BONILLO, 2013). O exemplo prático presente na plataforma, da mesma forma que o referido passo-a-passo, foi desenvolvido baseando-se nos vídeos "Como computadores quânticos quebram a criptografia (Algoritmo de Shor Explicado)"e "Como é possível o Algoritmo de Shor fatorizar 314191? | Minuto da Física", disponibilizados pelo canal Minuto da Física (2019).

Os módulos que constam no segundo bloco de estudos da plataforma, bloco responsável, conforme visto, por abordar o Algoritmo de Shor, seguem uma ordenação que foi desenvolvida com base no próprio passo-a-passo de execução do algoritmo. O modo de apresentação dos conteúdos presentes em cada módulo foi inspirado nos vídeos mencionados no início da seção 4.2, bem como o exemplo prático apresentado, cujos valores matemáticos são encontrados em um dos vídeos utilizados como referência. O ponto de partida é um módulo que trata de conceituar o Algoritmo de Shor, ambientando o estudante a ele. Na sequência, iniciam-se os módulos que tratam de apresentar o funcionamento do algoritmo. A figura 2 apresenta o fluxograma de funcionamento deste bloco, e a figura 3 mostra um dos exercícios presentes na plataforma sobre o Algoritmo de Shor.

Para percorrer os slides, o usuário conta com a presença das setas localizadas nas laterais da apresentação, podendo avançar ou voltar as lâminas. Os blocos de estudo foram desenvolvidos no modelo de carrossel, permitindo que o usuário, ao chegar na lâmina final, possa retornar à lâmina inicial apenas clicando na seta localizada à direita da tela. A tela final conta com um botão que possibilita retornar para a tela inicial da Hello Shor!. O site conta também com uma animação estilizada de caixas flutuantes ao fundo da tela, que movimentam-se para cima. Esta animação, além de possibilitar a transmissão da ideia de dinamismo, aprimora o design da

Figura 2 – Segundo Bloco de Estudos da Hello Shor!



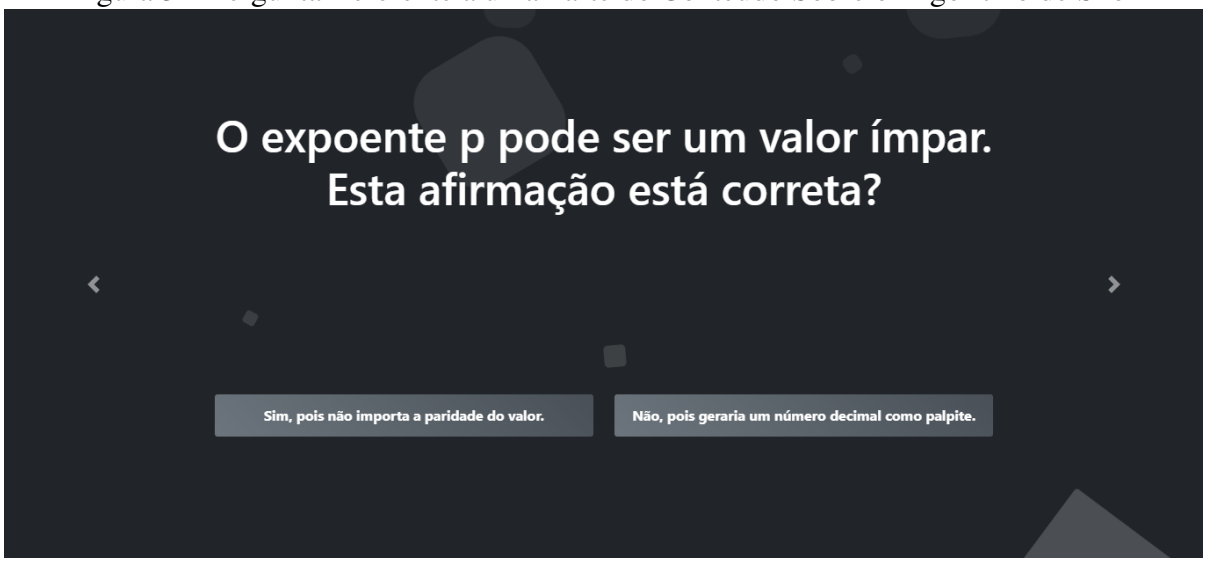
Fonte: Autoral

plataforma, colaborando com a eficiência dela.

4.2.1 Tecnologias Envolvidas

Para o desenvolvimento da Hello Shor!, utilizou-se a linguagem de marcação HTML, estilizada com o uso do CSS. O framework Bootstrap também está presente na implementação da plataforma, sendo atuante na manipulação dos elementos do documento HTML. Fez-se uso do Bootstrap, inclusive, para a estruturação dos slides no formato de carrossel, que permite ao usuário avançar até o final dos slides e retornar ao início da apresentação do conteúdo do site,

Figura 3 – Pergunta Referente a uma Parte do Conteúdo Sobre o Algoritmo de Shor



Fonte: Autoral

caso, então, avance uma lâmina a mais. A Hello Shor! vale-se também da disponibilização de modais, elaboradas com as tecnologias mencionadas, que visam o fornecimento de um feedback ao usuário após ele responder uma pergunta proposta por ela, informando se ele acertou ou não a resposta. A figura 4 ilustra a codificação da plataforma, apresentando um de seus trechos, sendo este escrito para a explicação sobre parte do funcionamento do Algoritmo de Shor.

A implementação do site utilizou, sobretudo, em concordância com o que foi relatado anteriormente, tecnologias de desenvolvimento frontend, e por esta razão, inicialmente, não é necessário que os dispositivos em geral tenham alguma configuração específica de hardware para o carregamento da plataforma. Os dispositivos somente necessitam estar conectados à internet para que seja possível a execução da Hello Shor!. É possível efetuar o acesso à plataforma educativa por meio do uso dos navegadores Google Chrome e Mozilla Firefox. Destaca-se que a Hello Shor! não apresenta delay ao ser carregada, e tampouco há atraso quando se avançam as lâminas por ela compreendidas.

Figura 4 – Código HTML Utilizado para a Explicação sobre Parte do Funcionamento do Algoritmo de Shor

```
<div class="carousel-item">
    <div class="carousel-caption">
        <h4>Todavia, é bastante improvável que, ao fatorar um número muito grande, o
            primeiro palpite seja um número que compartilhe fatores com N. Então, o Algoritmo de
            Shor
            efetua a melhoria deste palpite, buscando um melhor valor para a fatoração do número N.
        </h4>
    </div>
</div>
```

Fonte: Autoral

4.3 Metodologia de Avaliação

A metodologia de avaliação empregada pelo presente artigo foi feita em duas etapas: Uma pesquisa de satisfação e um questionário de avaliação sobre o aprendizado do conteúdo. Esta metodologia valeu-se, inicialmente, da aplicação da plataforma em 10 usuários convidados que já tenham cursado ou estejam cursando algum curso relacionado à área da computação, visando atender ao público-alvo, mencionado na subseção 4.1. Também foi verificado antes da aplicação da Hello Shor! que os usuários participantes desconheciam ou pouco conheciam a computação quântica ou o Algoritmo de Shor, o que foi importante para a avaliação da eficácia da plataforma: Como os estudantes não tinham conhecimento sobre o algoritmo, foi possível oportunizar a apresentação deste a eles, indo ao encontro do objetivo da Hello Shor!.

4.3.1 Utilização da Plataforma e Pesquisa de Satisfação

A primeira parte da aplicação da metodologia de avaliação, conforme mencionado anteriormente, consistiu na utilização da plataforma Hello Shor! por parte dos estudantes. Na ocasião, eles foram convidados a fazerem uso da plataforma sem instruções prévias técnicas sobre o Algoritmo de Shor. A ideia, neste cenário, é que eles interagissem com a Hello Shor! visando aprender sobre o que é o Algoritmo de Shor e a sua aplicação, o que é o intuito da plataforma. Os estudantes também receberam a informação de que, após a utilização da Hello Shor!, seria realizada uma pesquisa de satisfação, contendo perguntas a respeito da avaliação do usuário sobre ela.

Uma vez que os estudantes utilizaram a plataforma Hello Shor!, eles responderam a uma pesquisa de satisfação. Esta pesquisa indagava sobre qual curso o estudante está atualmente cursando ou já cursou, com opções de resposta mencionando cursos relacionados à área da computação. Perguntou-se, também, sobre qual a escolaridade do estudante, entre ensino superior incompleto e ensino superior completo. Foi questionado também se o estudante aprova a Hello Shor! para o ensino do Algoritmo de Shor, respondendo "Sim"ou "Não". Além disto, de maneira a detalhar a avaliação da plataforma, foi solicitada uma nota de 0 a 10 sobre à utilização dela.

4.3.2 Questionário de Avaliação Sobre o Aprendizado do Conteúdo

Os estudantes também foram convidados a participar de um questionário de avaliação sobre o aprendizado do conteúdo. Este questionário tinha o objetivo de avaliar a eficácia da Hello Shor! quanto ao seu propósito, que é a apresentação do Algoritmo de Shor a iniciantes. Foram elaboradas 5 questões de múltipla escolha que retomam o conteúdo apresentado pela plataforma: Primeiramente, perguntou-se, em última análise, sobre o que é a sobreposição quântica. Após isto, foi questionado qual é o objetivo do Algoritmo de Shor. Na sequência, tratou-se

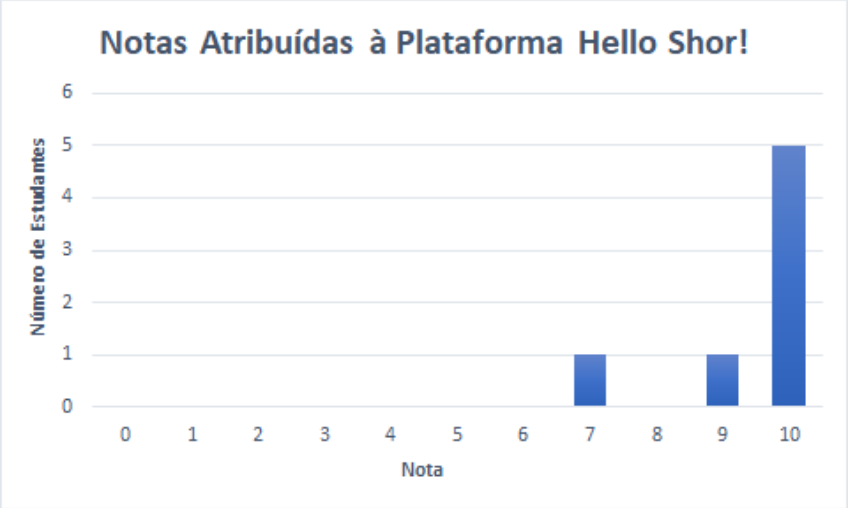
de perguntar, em resumo, sobre o motivo que leva ao RSA ser vulnerável ao algoritmo quântico apresentado pela plataforma. Em seguida, indagou-se qual é a função da Transformada Quântica de Fourier no Algoritmo de Shor. Por fim, foi questionada qual é a saída do referido algoritmo quântico.

5 RESULTADOS

Os resultados apresentados na presente seção foram obtidos após a aplicação da metodologia de avaliação relatada na subseção 4.3. Verificou-se que, dos 10 estudantes convidados a utilizar a plataforma Hello Shor! e a responder às pesquisas, 7 o fizeram. Como o mínimo esperado eram 5 estudantes, considera-se 7 como um número satisfatório. Dentre os usuários participantes do processo avaliativo, 3 estudam o curso de Ciência da Computação na Universidade do Vale do Rio dos Sinos (UNISINOS), 1 estuda o mesmo curso na Universidade Federal do Rio Grande do Sul (UFRGS), 2 estudam Análise e Desenvolvimento de Sistemas na UNISINOS e 1 é graduado em Sistemas de Informação pela UNISINOS. De acordo com estes dados, todos os usuários estão estudando ou já estudaram algum curso relacionado à area da computação, compreendendo a ideia do público-alvo deste artigo, conforme consta na subseção 4.1.

Na pergunta referente à aprovação da plataforma Hello Shor! para o ensino do Algoritmo de Shor, todos os usuários responderam de forma afirmativa. Mais adiante, quando solicitado aos usuários uma nota de 0 a 10 em relação à plataforma em si, os resultados foram os seguintes: 1 voto foi para a nota 7, 1 para a nota 9 e 5 para a nota 10. Ao final, a média das notas foi de 9,43 pontos. Tendo em vista que todos os usuários aprovaram a plataforma, e que a média das notas superou os 9 pontos, infere-se que a plataforma foi eficiente em seu propósito, visto que os usuários demonstraram-se satisfeitos. A figura 5 aponta, graficamente, a disposição dos dados apresentados.

Figura 5 – Gráfico das Notas Fornecidas pelos Estudantes à plataforma Hello Shor!



Fonte: Autoral

Após a utilização da plataforma, foram recebidos feedbacks de alguns dos usuários que participaram da metodologia de avaliação. Dentre os feedbacks, um deles sugeria a implementação de uma barra de progresso na plataforma, que mostrasse ao usuário o quanto ele já avançou dentro do passo-a-passo educativo promovido pelo Hello Shor!. Outro feedback trouxe a ideia de permitir que o usuário possa avançar as lâminas da plataforma utilizando as setas do teclado. Todos os feedbacks recebidos foram positivos, e alguns deles, conforme os exemplos apontados, sugeriam melhorias na plataforma, o que pôde colaborar para uma melhor percepção a respeito dos pontos onde o Hello Shor! pode ser aprimorado, possibilitando o aumento de sua eficiência em apresentar o Algoritmo de Shor.

Os 7 estudantes também participaram do questionário de avaliação sobre o aprendizado do conteúdo, que tinha como objetivo avaliar a eficácia da plataforma Hello Shor! em apresentar o Algoritmo de Shor a iniciantes. Para a composição deste questionário, foram elaboradas 5 perguntas, sendo que a primeira dizia respeito ao bloco 1 de estudos, que objetiva efetuar uma introdução à computação quântica, e as 4 perguntas seguintes ao bloco 2, que tem o intuito de apresentar o algoritmo. Foram feitas mais perguntas a respeito do conteúdo presente no segundo bloco de estudos pelo fato de que ele aborda, diretamente, o Algoritmo de Shor, que é o tema da plataforma.

Verificou-se que todos os usuários responderam corretamente às questões sobre a conceituação de sobreposição quântica e sobre o objetivo principal do Algoritmo de Shor. Em relação à indagação a respeito da função da Transformada Quântica de Fourier, 4 dos estudantes assinalaram a alternativa correta dentre as opções de resposta. Quanto à pergunta sobre o motivo que leva ao RSA ser vulnerável ao Algoritmo de Shor, 6 estudantes responderam corretamente, assim como para a pergunta sobre a saída do algoritmo quântico abordado pela Hello Shor!. Ao final, a média simples sobre os 5 pontos do questionário foi de 4,28 pontos. A figura 6 apresenta um gráfico que relaciona as questões ao número de estudantes que acertaram as respectivas alternativas corretas, onde a numeração das perguntas é a mesma presente na lista a seguir, cujos itens em negrito são as respostas certas:

1. Qual operação da computação quântica caracteriza o qubit nos dois estados ao mesmo tempo, 0 e 1, formando o terceiro estado 0 + 1?

    - Medição
    - **Sobreposição**
    - Entrelaçamento
    - Ligação

2. Qual é o objetivo principal do Algoritmo de Shor?

    - **Efetuar a fatoração prima de números inteiros**
    - Ordenar uma lista de valores

- Aumentar o desempenho da operação de busca em largura
- Aumentar o desempenho da operação de busca em profundidade

3. Considerando, para esta questão, a criptografia RSA-2048 bits, por que é correto afirmar que o Algoritmo de Shor poderia quebrá-la, se executado em uma máquina quântica suficientemente robusta para isto?

   - Porque o Algoritmo de Criptografia RSA utiliza a operação de busca em largura para compor a chave pública
   - **Porque o Algoritmo de Criptografia RSA utiliza o problema da fatoração prima para compor a chave pública**
   - Porque o Algoritmo de Criptografia RSA é sensível à operação de medição de qubits, que pode recuperar facilmente o valor da chave pública
   - Porque o Algoritmo de Criptografia RSA utiliza a operação de busca em profundidade para compor a chave pública

4. Em resumo, qual o objetivo a Transformada Quântica de Fourier dentro do Algoritmo de Shor?

   - Fatorar um número inteiro N
   - Quebrar o Algoritmo RSA
   - **Verificar a frequência em que determinados eventos acontecem**
   - Medir o valor final da sobreposições utilizadas para o cálculo de melhoria de palpites

5. Qual é a saída do Algoritmo de Shor, dado um número N de entrada?

   - **Os fatores do número N**
   - Uma sobreposição do número N
   - O número de nós percorridos no grafo em questão até localizar o número N
   - Uma lista de valores, formados pelos fatores de N, pelo número N e pelo tempo de execução do algoritmo

5.1 Discussão e Limitações

Os resultados da avaliação da eficácia da Hello Shor! mostram que os estudantes que participaram do processo demonstraram o entendimento sobre o Algoritmo de Shor conforme a expectativa inicial. Obteve-se um retorno muito satisfatório no que refere ao entendimento sobre a atuação do algoritmo para a fatoração prima de números inteiros, bem como a respeito se

Figura 6 – Relação entre as Perguntas da Avaliação da Eficácia da Hello Shor! com o Número de Estudantes que Acertaram as Respectivas Respostas

Fonte: Autoral

sua ação sobre o Algoritmo de Criptografia RSA, e a partir disso, infere-se que a plataforma é eficaz em atuar como ponto de partida nos estudos relacionados ao avanço do impacto da computação quântica sobre o RSA. Em adição, verificou-se que os estudantes demonstraram a compreensão referente à conceituação de sobreposição, conteúdo fundamental no estudo sobre o Algoritmo de Shor.

Considerando a média de 4,28 pontos sobre os 5 pontos do questionário, o valor do desvio padrão foi de 1,11 pontos. Para uma melhor análise de tal valor, cabe dizer que, dentre os 7 participantes da metodologia de avaliação da plataforma Hello Shor!, 4 deles acertaram todas as 5 questões, 2 assinalaram às alternativas exatas de 4 perguntas, e apenas 1 pessoa respondeu corretamente a somente 2 questões. Vistos estes dados, a maioria dos estudantes, apesar do valor de 1,11 pontos mostrado pelo desvio padrão, efetuaram a marcação de, no mínimo, 4 respostas certas, e desta forma, pode-se dizer que eles apresentaram um desempenho bastante satisfatório no preenchimento do questionário.

Todavia, há de se ressaltar que a questão onde ocorreram menos respostas certas foi a que trata da função da Transformada Quântica de Fourier no Algoritmo de Shor, e a partir disto, entende-se que uma ação de melhoria para a plataforma é aprimorar a elucidação do propósito da transformada. Tal melhoria pode ser promovida por meio da adição de exemplos sobre o funcionamento deste conteúdo, bem como pela inclusão de mais exercícios sobre ele. Com a implementação desta melhoria, e também das apontadas nos feedbacks mencionados anteriormente, entende-se que seriam necessários novos testes com outros estudantes, visando enriquecer a avaliação sobre a eficácia da plataforma, bem como de sua eficiência. Ainda assim, destaca-se que, nesta análise, a Hello Shor! cumpriu com o seu objetivo.

6 CONCLUSÕES E TRABALHOS FUTUROS

Desde o início da década de 2010 até a época atual, a ciência da computação vem apresentando resultados promissores quanto ao avanço do impacto da computação quântica sobre o algoritmo de criptografia RSA. Na base de pesquisas onde são mostrados estes resultados, nota-se a presença do Algoritmo de Shor. Uma maneira de colaborar para com estas pesquisas, infere-se, dada a referida presença do algoritmo quântico, é por meio da apresentação de estudantes a ele: Com um maior número de pessoas da área da computação conhecendo este algoritmo, possibilita-se a aproximação delas a tais pesquisas, e desta forma, estaria-se indo ao encontro da colaboração referenciada.

Neste sentido, é proposta uma plataforma educativa denominada Hello Shor!, que diferentemente das metodologias correlatas, apresenta o Algoritmo de Shor valendo-se de conceitos, exemplos e exercícios interativos. A plataforma tem como público-alvo o estudante iniciante em seu tema, compreendendo, mais especificamente, atuais estudantes do campo da computação e graduados em algum curso de tal campo, colocando em prática o pensamento de Paulo Freire (1992) sobre os diferentes conhecimentos já presentes em cada educando antes de uma prática pedagógica. Esta plataforma vem a ser um ponto de partida para o aprendizado sobre o Algoritmo de Shor, e consequentemente, para o progresso das pesquisas mencionadas no início desta seção.

O presente artigo, portanto, inclui na literatura um trabalho que aproxima a academia e pessoas vinculadas à area da computação às pesquisas referenciadas anteriormente. Há de se dizer que o referido artigo, com o intuito de atingir o seu objetivo, promove uma mescla entre a computação e fontes associadas à educação: Este trabalho embasou-se no pensamento de Paulo Freire (1992) na consideração dos conhecimentos prévios do estudante para a utilização da Hello Shor!, e na Teoria de Aprendizagem Significativa de David Ausubel (AGRA et al.; 2017) quando refere-se à construção de conhecimento ao longo do uso da plataforma, onde destaca-se o papel dos exercícios neste sentido. Estes embasamentos estão vinculados a fontes de um artigo que visa o ensino de um algoritmo de fatoração de números inteiros, o que evidencia a mescla estabelecida.

O trabalho é uma contribuição para a sociedade no sentido de que coopera para o desenvolvimento da computação quântica: Ele, por si próprio, possibilita a aproximação entre a categoria e estudantes acadêmicos do ramo da informática, bem como graduados em um curso que o compreenda. Reforça-se, nesta seção, o grande valor dos resultados da computação quântica para uma série de áreas de estudo, conforme apontou-se na introdução deste artigo, e visto isto, o aumento da proximidade mencionada muito contribui para o progresso da ciência. Este trabalho, assim sendo, passa a figurar na literatura como uma importante fonte no que se refere à computação quântica.

O artigo também convida a ciência da computação, em nível acadêmico, a valer-se da utilização de sua ideia: Desenvolver soluções para a área formada pela união entre a educação e a

tecnologia, objetivando a apresentação de conceitos de grande relevância, tendo como público-alvo estudantes iniciantes do tema. Tais soluções poderiam compreender, entre outros exemplos, a implementação de plataformas web e aplicativos de celular para a abordagem educativa do assunto em questão. Ações como esta são importantes para a ampliação da cooperação dos universitários com temas em destaque no campo da informática, o que permite colaborar para com o seu avanço.

Este trabalho, mesmo que tenha atingido o seu objetivo, possui algumas limitações, e dentre elas, há o fato de que a plataforma Hello Shor! não apresenta detalhes técnicos que tratam dos requisitos de ambiente necessários para que o Algoritmo de Shor possa ser implementado. O artigo também não visa a abordagem de uma possível promoção de uma metodologia de melhoria de funcionamento do algoritmo, uma vez que a sua área de atuação é a iniciação a ele. Também por conta da área de atuação relatada, o trabalho não tem como propósito efetuar a apresentação de dados históricos a respeito da evolução da aplicação do algoritmo quântico desde o seu lançamento.

Cita-se, como trabalho futuro, a implementação das sugestões de melhoria elaboradas pelos estudantes que participaram da metodologia de avaliação da plataforma Hello Shor!, presentes na seção de resultados. Em adição, há também a disponibilização do site em inglês, de maneira a efetuar a sua internacionalização. Com a plataforma disponível na lingua inglesa, mais pessoas ao redor do planeta poderiam ser beneficiadas com a ferramenta, e desta forma, um maior número de estudantes seriam aproximados às pesquisas referidas pela presente seção. Outra ideia para um trabalho futuro é incluir, na Hello Shor!, uma funcionalidade que incentive o estudante a utilizar linguagens de programação quânticas para a implementação do Algoritmo de Shor, dando dicas para tal ação.

O presente artigo promove, com sucesso, conforme visto em seu decorrer, uma metodologia pedagógica para a apresentação do Algoritmo de Shor a iniciantes. Os resultados obtidos com a avaliação da plataforma Hello Shor! mostram que ela é eficiente e eficaz em apresentar o algoritmo quântico para fatoração prima de números inteiros. O progresso da computação quântica sobre o algoritmo de criptografia RSA é favorecido com este trabalho, visto que ele é capaz de aproximar estudantes da área da computação às pesquisas relacionadas a tal avanço, o que pode permitir uma maior colaboração com elas, e consequentemente, beneficiar a ciência da computação.

Referências

ABUBAKAR, A. et al. **Cryptanalytic Attacks on Rivest, Shamir, and Adleman (RSA) Cryptosystem: Issues and Challenges.**, International Islamic University, Malásia, v. 61, n. 1, 2014.

AGRA, G. et al. **Análise do conceito de Aprendizagem Significativa à luz da Teoria de**

Ausubel, João Pessoa, Brasil: Revista Brasileira de Enfermagem, 2017. (REBEn), p. 1-2.

AMICO, M.; SALEEM, Z.; KUMPH, M. **An Experimental Study of Shor's Factoring Algorithm on IBM Q.** New York, NY: The Graduate School and University Center, The City University of New York, 2019. p. 1-8.

ATTUX, R. et al. **EE300 - Capítulo 5 - Equação de Schrödinger.** 2012. Disponível em: <http://www.dca.fee.unicamp.br/~attux/notas_cap5.pdf>. Acesso em: 30 março 2020.

BARRENO, M. **The Future of Cryptography Under Quantum Computers.** Hanover, NH: Dartmouth College Computer Science Technical Report, 2002. p. 28-29.

BERNSTEIN, D. et al. **Post-quantum RSA.** Chicago, IL: Department of Computer Science University of Illinois at Chicago, 2017. p. 1-2.

BLAKEY, E. **Factorizing RSA Keys, An Improved Analogue Solution.** Oxford, Oxon: Oxford University Computing Laboratory, 2009. p. 1-6, p. 19.

BONILLO, V. **Principios Fundamentales de Computación Cuántica** Espanha: Departamento de Computación - Facultad de Informática - IEEE, 2013. p. 140-143.

DATTANI, N.; BRYANS, N. **Quantum factorization of 56153 with only 4 qubits.** Kyoto, Japão: Quantum Chemistry Laboratory, Kyoto University, 2014. p. 1, p. 3.

DYAKONOV, M. **When will we have a quantum computer?.** Montpellier, França: Laboratoire Charles Coulomb, Université Montpellier, CNRS, 2019. p. 1-4, p. 8.

FREIRE, Paulo. **Pedagogia da Esperança**, Rio de Janeiro, Brasil: Editora Paz e Terra, 1992. Volume 11.

FREITAS, A.. **Algoritmo de Shor e sua aplicação à fatoração de números inteiros**, Belo Horizonte, Minas Gerais: Universidade Federal de Minas Gerais, 2010. (UFMG), p. 46-52, p. 59-60.

GELLER, M.; ZHOU, Z. **Factoring 51 and 85 with 8 qubits.** Athens, GA: E. L. Department of Physics and Astronomy, University of Georgia, 2013. p. 1-4.

GIDNEY, C.; EKERÅ, M. **How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.** Santa Barbara, CA: Google Inc., 2019. p. 1, p. 17, p. 20-21.

HAUKE, P. et al. **Perspectives of quantum annealing: Methods and implementations.** Heidelberg, Alemanha: Kirchho-Institute for Physics, Heidelberg University, 2019. p. 2.

JIANG, S. et al. **Quantum Annealing for Prime Factorization.** West Lafayette, IN: 1Department of Computer Science, Purdue University, 2018. p. 1.

KIRSCH, Z. **Quantum Computing: The Risk to Existing Encryption Methods.** Medford, MA: Tufts University, 2015. p. 7.

KLEINJUNG, T. et al. **Factorization of a 768-bit RSA modulus.** Lausanne, Suíça: EPFL IC LACAL, Station 14, CH-1015, 2010. p. 1-9, p. 13-14.

LONE, A. et al. **Common Attacks on RSA and its Variants with Possible Countermeasures.** International Journal of Emerging Research in Management & Technology., New Delhi, Índia, v. 5, n. 5, 2016.

MATSUURA, S. et al. **Quantum annealing correction at finite temperature: ferromagnetic p-spin models.** Copenhagen, Dinamarca: Niels Bohr International Academy and Center for Quantum Devices, Niels Bohr Institute, Copenhagen University, Blegdamsvej 17, 2016. p. 1.

MAVROEIDIS, V. **The Impact of Quantum Computing on Present Cryptography.** Oslo, Noruega: Department of Informatics, University of Oslo, 2018. p. 1-4, p. 8.

MENGONI, et al.; **Breaking RSA Security With A Low Noise D-Wave 2000Q Quantum Annealer: Computational Times, Limitations And Prospects** Bologna, Itália: CINECA, 2020. p. 1-3.

MICROSOFT. **Quantum.** Disponível em: <https://github.com/microsoft/Quantum> Acesso em 15 ago. 2020.

MILANOV, E. **The RSA Algorithm.** Washington, DC: Department of Mathematics, University of Washington, 2009. (UW) p. 1.

MINUTO DA FÍSICA. **Como computadores quânticos quebram a criptografia (Algoritmo de Shor Explicado).** Disponível em: <https://www.youtube.com/watch?v=jA2FxG95iU8> Acesso em 28 set. 2020.

MINUTO DA FÍSICA. **Como é possível o Algoritmo de Shor fatorizar 314191? | Minuto**

da Física. Disponível em: <https://www.youtube.com/watch?v=9PgFqnOCscA> Acesso em 28 set. 2020.

NISHA, S.; FARIK, M. **RSA Public Key Cryptography Algorithm - A Review.**, International Journal of Scientific & Technology Research, Malásia, v. 61, n. 1, 2014.

ONODERA, T.; NG, E.; MCMAHON, P. **A quantum annealer with fully programmable all-to-all coupling via Floquet engineering.** Stanford, CA: E. L. Ginzton Laboratory, Stanford University, 2019. p. 1.

PAMPLONA, S. **Aplicação da Computação Quântica na Resolução de Problemas Computacionais e seu Impacto no Âmbito Científico.** Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/aplicacao-computacao-quantica-na-resolucao-problemas-computacionais-impacto-cientifico.htm> Acesso em 03 nov 2020.

PENG, W. et al. **Factoring larger integers with fewer qubits via quantum annealing with optimized parameters.** Shanghai, SH: Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai Institute for Advanced Communication and Data Science, Shanghai University, 2019. p. 1, p. 7.

PERLNER, R. et al. **Quantum Resistant Public Key Cryptography: A Survey.** Gaithersburg, MD: National Institute of Standards and Technology, 2009. p. 1.

RESCH, S.; KARPUZCU, U. **Quantum Computing: An Overview Across the System Stack.** Minneapolis, MN: University of Minnesota, 200 Union St SE, 2019. p. 1.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.** Cambridge, MA: Laboratory for Computer Science, Massachusetts Institute of Technology, 1977. p. 1-14.

SHOR, P. **Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.** Murray Hill, NJ: AT&T Research, Room 2D-149, 600 Mountain Ave, 1996. p. 1-5, p. 15, p. 24-25.

SOUSA, J. **Teste de robustez de chaves RSA.** Brasília, DF: Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília, 2016. p. 12.

WATSON, G. **Blue for trust, red for passion: how to pick a colour scheme for your brand.**

Disponível em: <https://www.theguardian.com/small-business-network/2015/aug/24/how-pick-colour-scheme-for-brand> Acesso em 28 set 2020.

WICAKSONO, A.; WICAKSANA, A. **Implementation of Shor's Quantum Factoring Algorithm using ProjectQ Framework.** Tangerang, Indonésia: International Journal of Engineering and Advanced Technology, 2019. (IJEAT) p. 1.

WOLF, R. **Quantum Computing: Lecture Notes.** Amsterdam, Holanda: QuSoft, CWI and University of Amsterdam, 2019. p. 35, p. 119.

XU, N. **Quantum Factorization of 143 on a Dipolar-Coupling NMR system.** Hefei, AH: Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, 2011. p. 1.