**UNIVERSIDADE PRESBITERIANA MACKENZIE**

FACULDADE DE COMPUTAÇÃO E INFORMÁTICA

Bryan Kano Ferreira

Daniel Ricardo Ghirghi

Marcelo Batista De Lima Junior

Análise de vulnerabilidades e aprimoramento do protocolo quântico de troca de chaves criptográficas BB84.

SÃO PAULO

2019

Bryan Kano Ferreira

Daniel Ricardo Ghirghi

Marcelo Batista De Lima Junior

Análise de vulnerabilidades e aprimoramento protocolo quântico de troca de chaves criptográficas BB84.

Projeto do Trabalho de Conclusão de Curso apresentado à Faculdade de Computação e Informática da Universidade Presbiteriana, desenvolvida como requisito parcial para aprovação na disciplina de Metodologia da Pesquisa em Computação, ministrada pelo professor Dr. Everton Knihs, do curso de ciência da computação.

Orientador: Pr. Dr. Luciano Silva

SÃO PAULO

2019

**RESUMO**

No cenário atual, em que as pesquisas relacionadas a computação quântica estão em alta, e as tecnologias que permitem realizar isso na prática estão tendo uma grande evolução, os dados sigilosos em sistemas, como por exemplo senhas ou dados pessoais, da maneira como são armazenadas e protegidos atualmente, são vulneráveis contra o ataque de força bruta de computadores quânticos, portanto o objetivo deste trabalho de TCC é aprimorar o protocolo de distribuição de chaves quânticas BB84, que é utilizado atualmente mas possui uma vulnerabilidade quando se trata de ataques de força bruta de computadores quânticos, a principio essa vulnerabilidade deverá ser testada e analisada e em seguida deverá ser proposta, testada e analisada uma solução de implementação para mitigar essa vulnerabilidade, utilizando a máquina quântica IBM Q durante esses processos.

**Palavras-chave:** Computação, Quântica, Criptografia, Chaves, BB84

**ABSTRACT**

In the current scenario, where research related to quantum computing is on the rise, and the technologies that allow it to do so in practice are evolving, sensitive data in systems, such as passwords or personal data, as it is stored and currently protected, are vulnerable against the brute force attack of quantum computers, so the purpose of this undergraduate final work is to enhance the BB84 quantum key distribution protocol, which is currently used but has a vulnerability when it comes to brute force attacks of quantum computer systems. At first this vulnerability will be tested and analyzed and then an implementation solution will be proposed, tested and analyzed to mitigate this vulnerability, using the IBM Q quantum machine during these processes.

**Key-words:** Computing, Quantum, Cryptography, Keys, BB84

**SUMÁRIO**

1. **INTRODUÇÃO.......................................................................................5**

1.1 CONTEXTUALIZAÇÃO E RELEVÂNCIA DO TEMA.......................5

1.2 OBJETO DE PESQUISA.................................................................5

1.2.1 PROBLEMA DE PESQUISA..............................................5

1.2.2 HIPÓTESE.........................................................................5

1.2.3 VARIÁVEIS........................................................................6

1.2.4 VARIÁVEIS........................................................................6

1.3. OBJETIVOS DO ESTUDO.............................................................6

1.3.1 OBJETIVO GERAL............................................................6

1.3.2 OBJETIVOS ESPECÍFICOS..............................................6

1.4 JUSTIFICATIVA...............................................................................6

1.5 DELIMITAÇÃO DO ESTUDO .........................................................7

1.6 ORGANIZAÇÃO DO ESTUDO........................................................7

1. **REFERENCIAL TEÓRICO………………...............................................8**
2. **METODOLOGIA DA PESQUISA………………………………………….9**
3. **CRONOGRAMA ...................................................................................11**

**REFERÊNCIAS.....................................................................................12**

**1. INTRODUÇÃO**

* 1. **CONTEXTUALIZAÇÃO E RELEVÂNCIA DO TEMA**

As pesquisas relacionadas a computação quântica vêm evoluindo muito nos últimos anos, ao mesmo ritmo em que grandes empresas como Google, IBM e Microsoft começaram a investir na construção e aprimoramento de seus respectivos computadores quânticos, o que indica uma grande chance de que no futuro esses computadores com alta capacidade de processamento sejam produzidos em maior escala, sendo assim, é necessário que as consequências do aparecimento de uma tecnologia tão poderosa no mercado sejam analisadas. Uma das consequências mais relevantes e observáveis é o fato de que, com o grande potencial computacional de um computador quântico, a criptografia usada atualmente para proteger dados sigilosos como senhas de usuários ou informações confidenciais armazenadas nos sistemas de empresas se tornam ineficazes, visto que com um ataque de força bruta um computador quântico é capaz de quebrar esse nível de criptografia em um tempo extremamente menor do que um computador convencional. Portanto, é necessário que sejam criados, ou aprimorados os algoritmos e esquemas existentes de criptografia.

**1.2 OBJETO DE PESQUISA**

**1.2.1 PROBLEMA DE PESQUISA**

Com o advento da computação quântica, o protocolo quântico de troca de chaves criptográficas BB84 fica vulnerável ao ataque de força bruta de computadores quânticos.

Neste contexto, a pergunta que será respondida nesta pesquisa é:

É possível aprimorar o esquema BB84 para que se torne mais resistente à ataques de força bruta disparados por computadores quânticos?

**1.2.2 HIPÓTESE**

Sim, o protocolo quântico de troca de chaves criptográficas BB84 é vulnerável ao ataque de força bruta de computadores quânticos e pode se tornar mais resistente adicionando ruídos no canal de comunicação através de covariâncias de laser na fibra ótica que não fazem parte da informação, obfuscando o conteúdo real, dessa forma mesmo que o atacante consiga obter a chave adicionada de ruídos através de força bruta, ela não terá utilidade já que para utilizá-la precisará saber também os parâmetros para encontrar a informação real.

**1.2.3 VARIÁVEIS**

Inicialmente temos duas variáveis:

Uma variável booleana que determina se a solução a ser encontrada e implementada neste trabalho tornou o protocolo BB84 mais resistente.

Uma variável quantitativa que determina em valores matemáticos o quanto a solução a ser encontrada e implementada tornou o protocolo BB84 mais resistente e eficiente.

**1.3 OBJETIVOS DO ESTUDO**

**1.3.1 OBJETIVO GERAL**

O presente trabalho tem por objetivo geral tornar o protocolo quântico de troca de chaves criptográficas BB84 mais resistente à ataques de força bruta de computadores quânticos.

**1.3.2 OBJETIVOS ESPECÍFICOS**

Sobre os Objetivos Específicos tem-se:

Simular um ataque de força bruta ao esquema quântico de chaves criptográficas BB-84 utilizando a máquina quântica fornecida pela IBM e analisar os resultados.

Por fim, encontrar uma maneira de aprimorar o esquema BB-84 para que se torne pós-quântico.

# 1.4 JUSTIFICATIVA

O aprimoramento de esquemas criptográficos com o constante avanço dos computadores quânticos é de extrema urgência.

Com o poder de processamento de um computador quântico é possível quebrar em algumas horas uma senha criptografada, que com um computador normal levaria dias ou até meses.

Atualmente, o custo de um computador quântico torna sua aquisição impossível para usuários comuns, e só empresas de grande porte possuem declaradamente essa tecnologia. Porém, como toda tecnologia no mercado, ela tende a se tornar mais barata com o passar do tempo, e uma vez que essa tecnologia tenha um custo mais acessível, todo o cenário da criptografia no mundo deve mudar, visto que serão necessárias técnicas e algoritmos muito mais sofisticados para manter a segurança, levando em consideração o poder computacional dos novos atacantes.

Portanto, esse TCC visa contribuir para a segurança da informação em um cenário futuro, aprimorando o protocolo quântico de troca de chaves criptográficas BB84 para que ele se torne mais eficaz contra os ataques de força bruta de computadores quânticos.

# DELIMITAÇÃO DO ESTUDO

Este trabalho possui uma delimitação temporal, visto que a tecnologia avança a cada dia, eventualmente o esquema aprimorado se tornará obsoleto novamente, devido ao surgimento de novas técnicas e tecnologias, exigindo assim atualizações, portanto o tempo pelo qual essa solução é viável depende de fatores externos, mas ela se provará relevante no mínimo durante alguns anos após a massificação dos computadores quânticos.

**1.6 ORGANIZAÇÃO DO ESTUDO**

Este projeto de Trabalho de Conclusão de Curso (TCC) está organizado em 4 capítulos conforme descritos a seguir:

O capítulo 1 contempla a introdução do trabalho, apresentando a relevância do tema, o problema da pesquisa, o objetivo geral e os específicos, a delimitação do estudo e sua organização.

O capítulo 2 contempla o referencial teórico, apresentando sínteses e relacionamentos dos conteúdos das referências utilizadas durante o estudo.

O capítulo 3 contempla a metodologia da pesquisa, indicando as técnicas a serem utilizadas e seus respectivos motivos de escolhas, apresentando as etapas e classificação da pesquisa.

O capítulo 4 contempla a divisão temporal das etapas metodológicas definidas no capítulo anterior, apresentando o cronograma do trabalho.

**2. REFERENCIAL TEÓRICO**

Este referencial teórico foi obtido através de autores como Noson S. Yanofsky, Mirco A. Mannucci, Dilip Kumar Shaw e Kausik Saha, além de pesquisas em periódicos científicos, sites, teses e dissertações em universidades.

No livro “Quantum Computing for Computer Scientists” o material é organizado para

analisar diferentes aspectos da computação quântica do ponto de vista específico da ciência da computação, com capítulos sobre arquitetura de computadores,

algoritmos, linguagens de programação, criptografia etc.

O livro “Quantum Key Distribution Scheme based on BB84 Protocol” trata do conceito da criptografia quântica, os vários protocolos usados ​​na distribuição de chaves quânticas e a análise dos mesmos, com foco no protocolo BB84 e sua implementação.

O livro “Handbook of Applied Cryptography” fornece uma introdução aos aspectos mais práticos da criptografia convencional, apresentando as mais conhecidas técnicas e algoritmos.

O artigo “Quantum key distribution over 67 km with a plug&play system” apresenta um sistema de distribuição de chaves quânticas com fibra óptica, apresenta detalhes sobre o canal de comunicação utilizado na distribuição de chaves quânticas e trata de questões relacionadas a infraestrutura, simulando uma troca de chaves entre Genebra e Lausanne, testando a estabilidade em condições de campo.

O artigo “A quick glance at quantum cryptography” aborda conceitos gerais sobre criptografia quântica, sobre a infraestrutura utilizada nesse modelo, algoritmos e diversos protocolos de troca de chaves quânticas, inclusive o BB84.

**3. METODOLOGIA DA PESQUISA**

Com relação a metodologia utilizada neste TCC, o trabalho terá início com a leitura do livro “Quantum Computing for Computer Scientists”, que aborda os conceitos básicos para que seja possível lidar com o tema da pesquisa, após isso serão buscadas outras fontes com conteúdo mais específico. O foco da leitura abrangerá conceitos da matemática com números complexos, cujo conhecimento é necessário visto que é a base da computação quântica, e abordará também questões mais específicas como linguagens de programação e criptografia.

A leitura, análise e comparação da fundamentação teórica terá como objetivo a busca de conhecimento a respeito da computação quântica e como seria possível melhorar os algoritmos existentes de criptografia para que se tornem resistentes a ataques de força bruta, nesse caso com foco no BB84, para resolver o problema da ameaça à segurança da informação que tende a surgir com o avanço da tecnologia e presença de computadores quânticos poderosos no mercado.

A metodologia utilizada nesta pesquisa compreende também um estudo e testes práticos utilizando o computador quântico fornecido pela IBM, para provar inicialmente a existência dessa vulnerabilidade em relação aos ataques de força bruta, e posteriormente como nossa solução a ser proposta e que será implementada em uma linguagem de programação, se provará eficiente nesse cenário.

Durante a realização do projeto, serão armazenados dados de execução no computador quântico que serão analisados, essa análise gerará uma série de indicadores, envolvendo gráficos de eficiência, velocidade, custo computacional, entre outras. Em seguida, serão extraídas algumas conclusões dessas análises, que serão checadas por meio de ferramentas específicas.

Como resultado, será apresentada uma solução eficaz e eficiente para resolver o problema de pesquisa, que é aprimorar o protocolo BB84, e serão geradas conclusões finais, que serão documentadas no texto final do TCC.

Assim, pode-se dizer que as seguintes etapas deverão ser desenvolvidas nesse estudo:

1 - Revisão sistemática de artigos sobre computação quântica e criptografia pós-quântica.

2 - Simulação de um ataque de força bruta ao protocolo de distribuição de chaves quânticas BB84 na máquina IBM Q.

3 - Análise dos resultados da simulação.

4 - Aprimoramento pós-quântico do protocolo de distribuição de chaves quânticas BB84.

5 - Simulação de um ataque de força bruta ao protocolo de distribuição de chaves quânticas BB84 aprimorado na máquina IBM Q.

6 - Análise dos resultados da simulação.

7 - Criação do artigo final do TCC

Em termos de classificação desta pesquisa, segundo os enfoques clássicos de

classificação de uma pesquisa científica, entende-se que esta pode ser

enquadrada conforme se apresenta na sequência.

Quanto à Natureza, esta é uma pesquisa Aplicada, já que sua aplicação

prática é imediata.

Quanto à Forma de Abordagem, a pesquisa pode ser considerada quantitativa, uma vez que desenvolve técnicas quantitativas.

Quanto aos Fins (finalidades), a pesquisa é metodológica, já que

apresenta uma metodologia de trabalho, inclusive com o desenvolvimento

de um algoritmo e um programa em linguagem de programação.

Quanto aos Meios (recursos empregados na pesquisa), foram utilizados

os seguintes recursos: Bibliografia, Dados Documentais e testes em infraestruturas de computadores quânticos disponibilizadas pela IBM.

Na pesquisa de laboratório, os dados serão levantados e testados em um período de 5 meses, utilizando os computadores quântico fornecidos virtualmente pela IBM e computadores pessoais para testes controlados.

**4. CRONOGRAMA**

As atividades desta pesquisa deverão ser desenvolvidas de acordo com o cronograma apresentado a seguir:

**Cronograma de Atividades**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ATIVIDADE** | **MÊS** | | | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| 1. Revisão sistemática de artigos sobre computação quântica e criptografia pós-quântica. |  |  |  |  |  |  |  |  |  |  |  |  |
| 2. Simulação de um ataque de força bruta ao protocolo de distribuição de chaves quânticas BB84 na máquina IBM Q. |  |  |  |  |  |  |  |  |  |  |  |  |
| 3. Análise dos resultados da simulação. |  |  |  |  |  |  |  |  |  |  |  |  |
| 4. Aprimoramento pós-quântico do esquema quântico de troca de chaves criptográficas BB84. |  |  |  |  |  |  |  |  |  |  |  |  |
| 5. Simulação de um ataque de força bruta ao protocolo de distribuição de chaves quânticas BB84 aprimorado na máquina IBM Q. |  |  |  |  |  |  |  |  |  |  |  |  |
| 6. Análise dos resultados da simulação. |  |  |  |  |  |  |  |  |  |  |  |  |
| 7. Criação do artigo final do TCC |  |  |  |  |  |  |  |  |  |  |  |  |

**REFERÊNCIAS**

YANOFSKY, Noson S.; MANNUCCI, Mirco A. **Quantum Computing for Computer Scientists**. 1. ed. New York, NY, USA: Cambridge University Press, 2008. 368 p. ISBN 0521879965 9780521879965.

SHAW, Dilip K.; SAHA, Kausik. **Quantum Key Distribution Scheme based on BB84 Protocol**. Letônia: LAP LAMBERT Academic Publishing, 2019. 52 p. ISBN 6139999804.

MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott **A. Handbook of Applied Cryptography: Discrete Mathematics and Its Applications**. 1. ed. USA: CRC Press, 1996. 780 p. ISBN 0-8493-8523-7.

TUCKI, D; GISIN, N; GUINNARD, O; RIBORDY, G; ZBINDEN, H. **Quantum key distribution over 67 km with a plug&play system**, Genebra, 2002. Disponível em: https://iopscience.iop.org/article/10.1088/1367-2630/4/1/341/pdf. Acesso em: 8 nov. 2019.

LOMONACO, Samuel J. **A Quick Glance at Quantum Cryptography**. Cryptologia, Baltimore County, MD, USA, 1999.