Universidade Tecnológica Federal do Paraná – UTFPR
Campus Toledo

Coordenação do Curso de Tecnologia em Sistemas para Internet

PRÉ-PROPOSTA DE TRABALHO DE TCC

SEGURANÇA EM COMUNICAÇÕES PÓS-QUÂNTICAS

Aluno: João Pedro Rodrigues Leite

Orientador: Prof. Dr. Fábio Engel de Camargo

Toledo
2024

Contexto

No contexto atual da segurança da informação, há uma crescente preocupação com a possível ameaça representada pelos computadores quânticos à criptografia convencional. À medida que a pesquisa e o desenvolvimento de tecnologia quântica avançam, torna-se cada vez mais claro que algoritmos de criptografia atualmente considerados seguros podem ser quebrados de forma eficiente por esses dispositivos computacionais revolucionários. Nesse cenário, surge a necessidade de explorar e desenvolver novas técnicas criptográficas que sejam resistentes aos ataques quânticos, dando origem ao campo emergente da criptografia pós-quântica. A segurança em comunicações pós-quânticas se torna, então, uma área de extrema importância, pois busca garantir a confidencialidade, autenticidade e integridade das comunicações digitais em um ambiente onde a segurança convencional pode ser comprometida.

Problema

O problema central que este TCC pretende abordar é a necessidade de garantir a segurança das comunicações digitais em um cenário futuro onde os computadores quânticos podem comprometer a eficácia dos algoritmos de criptografia convencionais. Com a iminente chegada da computação quântica, os métodos tradicionais de criptografia baseados em fatores de dificuldade computacional podem se tornar vulneráveis a ataques que exploram o poder computacional massivo dos computadores quânticos. Diante desse desafio, é fundamental desenvolver e implementar novas técnicas criptográficas pós-quânticas capazes de resistir aos ataques quânticos previstos, garantindo assim a segurança das comunicações em um futuro incerto e complexo.

Objetivo Geral

O objetivo geral desse TCC é realizar uma pesquisa sobre as soluções existentes na área da segurança da informação em comunicações pós-quânticas. O foco será na pesquisa e apresentação dos algoritmos de criptografia pós-quântica atualmente disponíveis ou que estão em processo de pesquisa. A pesquisa pretenderá identificar e avaliar as principais técnicas de criptografia desenvolvidas para proteger as comunicações digitais contra potenciais ataques por computadores quânticos, fornecendo uma visão ampla do estado atual nesse campo.

Solução Proposta

A solução proposta neste TCC consiste na apresentação dos principais aspectos dos algoritmos de criptografia pós-quântica já desenvolvidos. Pesquisas sobre trabalhos relacionados serão realizados de modo a identificar os algoritmos relevantes e os fundamentos por trás destes algoritmos.

Resultado Esperado

Com base na pesquisa e na análise dos desafios discorridos pela iminente chegada dos computadores quânticos e as potenciais ameaças à criptografia convencional, o resultado esperado deste trabalho é compreender as técnicas das criptografias pós-quânticas existentes. Espera-se que essa pesquisa identifique e avalie os algoritmos de criptografia pós-quântica mais notáveis e eficazes disponíveis atualmente ou que ainda estão em processo de pesquisa, fornecendo uma visão ampla do estado atual nessa área emergente da segurança da informação e que o trabalho contribua para uma maior conscientização sobre a importância da segurança em comunicações pós-quânticas.