Segurança em comunicações Pós-Quânticas

João Pedro Rodrigues Leite

Orientador: Prof. Dr. Fábio Engel de Camargo
Universidade Tecnológica Federal do Paraná (**UTFPR**)
Curso de Sistemas para Internet

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Sumário

Contextualização

- Avanços significativos na computação quântica ameaçam a segurança da criptografia convencional.
- Computadores quânticos podem realizar operações em paralelo, explorando superposição e emaranhamento.
- Essa capacidade pode comprometer a confidencialidade e integridade das comunicações digitais.
- A criptografia pós-quântica (CPQ) emerge como uma resposta a essas ameaças.

História da Computação Quântica

- 1981: Richard Feynman propõe a ideia de um computador baseado em princípios quânticos.
- 1985: David Deutsch formaliza o conceito de um computador quântico universal.
- 1994: Peter Shor desenvolve um algoritmo quântico que ameaça a criptografia baseada em fatoração.
- 1996: Lov Grover apresenta um algoritmo quântico eficiente para busca em bases de dados.

Definição do Problema

- A estratégia “store now, decrypt later” é uma ameaça emergente.
- Dados criptografados hoje podem ser vulneráveis a futuros avanços na computação quântica.
- A necessidade de algoritmos que resistam a ataques quânticos é urgente.

Objetivo Geral

- Estudar e apresentar os problemas e soluções de criptografia pós-quântica existentes de uma maneira mais acessível e compreensível, a fim de garantir a segurança das comunicações digitais.

Objetivos Específicos

- Identificar e catalogar os principais algoritmos de criptografia pós-quântica.
- Avaliar as bases teóricas e contextos de aplicação desses algoritmos.
- Apresentar uma comparação sobre os algoritmos de criptografia pós-quântica entre si em termos de complexidade computacional e praticabilidade.
- Elaborar recomendações para desenvolvedores web sobre o uso de CPQ.

Metodologia

- Revisão bibliográfica sobre algoritmos de criptografia pós-quântica.
- Comparar os algoritmos em termos de desempenho e segurança.
- Desenvolvimento de recomendações para a adoção de CPQ em sistemas web.

Resultados Esperados

- Identificação dos algoritmos de CPQ mais promissores.
- Análise das vantagens e limitações desses algoritmos.
- Recomendações práticas para a implementação de CPQ em sistemas digitais.

Cronograma

- **Outubro (2024):** Revisão dos apontamentos da banca.
- **Novembro (2024):** Revisão bibliográfica e redação do projeto de TCC.
- **Dezembro (2024):** Defesa do projeto de TCC e início da escrita da monografia.
- **Janeiro (2025):** Continuação da escrita da monografia e elaboração da apresentação final.
- **Fevereiro (2025):** Finalização da monografia, preparação da apresentação, revisão geral do trabalho, e defesa final do TCC.

Conclusão

- A computação quântica representa uma ameaça real à segurança digital.
- A adoção de criptografia pós-quântica é essencial para garantir a proteção de dados no futuro.
- Este trabalho contribuirá para a compreensão e adoção de CPQ.