

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



- 1 Contextualização
- 2 Definição do Problema
- 3 Objetivos
- 4 Metodologia
- 5 Resultados Esperados
- 6 Cronograma
- 7 Conclusão

- 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

- Anos 80: 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.

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

Objetivos Específicos

- Identificar os principais algoritmos de criptografia pós-quântica.
- Analisar as bases teóricas e contextos de aplicação desses algoritmos.
- Elaborar recomendações para desenvolvedores web sobre o uso de CPQ.

- Revisão bibliográfica sobre algoritmos de criptografia pós-quântica.
- Análise comparativa dos algoritmos em termos de desempenho e segurança.
- Estudo de casos de aplicação de CPQ em ambientes reais.
- Desenvolvimento de diretrizes para a adoção de CPQ em sistemas web.

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

- Mês 1-2: Revisão bibliográfica
- Mês 3-4: Análise dos algoritmos de CPQ
- Mês 5: Estudo de casos
- Mês 6: Redação e 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, oferecendo soluções práticas e seguras.