Segurança em comunicações Pós-Quânticas

João Pedro Rodrigues Leite

Contexto

- Crescente preocupação com ameaça dos computadores quânticos à criptografia convencional.
- Necessidade de desenvolver técnicas criptográficas resistentes a ataques quânticos.
- Surgimento da criptografia pós-quântica para garantir segurança das comunicações digitais.

Problema

- Computadores quânticos podem comprometer algoritmos de criptografia convencionais.
- Necessidade de desenvolver e implementar técnicas criptográficas pós-quânticas.

Objetivo Geral

- Pesquisar soluções em segurança da informação para comunicações pós-quânticas.
- Foco em identificar e avaliar algoritmos de criptografia pós-quântica.

Solução Proposta

- Apresentar principais aspectos dos algoritmos de criptografia pós-quântica.
- Identificar algoritmos relevantes e seus fundamentos.

Resultado Esperado

- Compreensão das técnicas de criptografias pós-quânticas existentes.
- Identificação e avaliação dos algoritmos mais notáveis e eficazes.