APLICAÇÃO DA CRIPTOGRAFIA PÓS-QUÂNTICA

Uma análise de sistemas criptográficos resistentes ao algoritmo de Shor

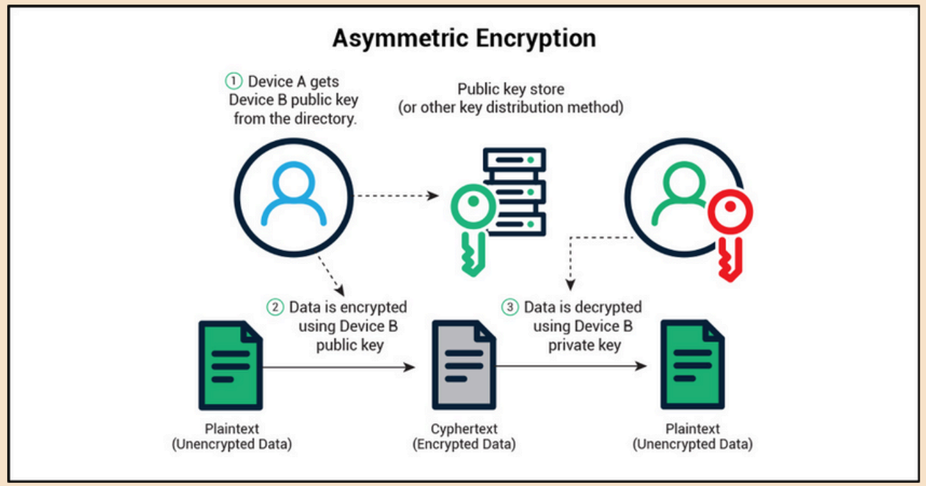
Isaque Barbosa

Orientador : Ramon Fontes

AMEAÇA QUÂNTICA À CRIPTOGRAFIA MODERNA

- Em 1994 Peter Shor propões um algoritmo capaz de resolver o problema da fatoração em tempo polinomial, a partir da redução ao problema do subgrupo oculto
- O problema da fatoração é presumido como suficientemente difícil de ser resolvido em computadores não quânticos e, por isto, é utilizados em algoritmos criptográficos de chave pública, como o *RSA*

- O Algoritmo RSA utiliza dois números primos para as chaves públicas e privadas
- Utiliza a chave pública para encriptação, e a privada para decriptação
- Com a fatoração polinomial, um atacante é capaz de derivar a chave privada e decriptar o texto



CRIPTOGRAFIAS PÓS-QUÂNTICAS

Dez 2016

O Instituto Nacional de Padrões e Tecnologia (NIST) inicia um programa, Post-Quantum Cryptography Standardization (PQC)[1], que visa padronizar algoritmos resistentes ao algoritmo de Shor

Jul 2022

O PQC seleciona, após três rodadas de submissões, o algoritmo CRYSTALS-Kyber para padronização

Nov 2022

Inicia-se uma quarta rodada do programa para novas análises com os algoritmos BIKE, Classic McEliece, HQC e SIKE

O projeto Open Quantum Safe (OQS), realizado pela *Linux Foundation*, busca reunir as implementações dessas criptografias em uma biblioteca implementada em C, chamada *liboqs*

1. https://csrc.nist.gov/Projects/post-quantum-cryptography

ANALISE SOBRE A APLICABILIDADE DOS ALGORITMOS

Após a implementação dos algoritmos, autores começaram a incorporá-los e analisá-los sobre os protocolos de comunicação utilizados na Internet, como o TLS e o Signal:

- Benchmarking Post-Quantum Cryptography in TLS, PAQUIN, C; STEBILA, D; TAMVADA, G. 2020. Que realizam e analisam uma implementação de algoritmos como SIKE e CRYSTALS-Kyber sobre o TLS
- Post-quantum key exchange for the TLS protocol from the ring learning with errors problem, BOS, J. W. 2015. Avalia a implementação de um algoritmo baseado no problema Ring Learning with Errors (R-LWE) sobre o TLS
- The Post-Quantum Signal Protocol Secure Chat in a Quantum World, DUITS, I. 2019. Apresenta uma análise de 11 algoritmos criptográficos, dentre eles o CRYSTALS-Kyber, sobre o Signal.

PROPOSTA DE TRABALHO

- Realizar revisão do estado da arte sobre computação quântica;
- Identificar os principais algoritmos de criptografia pós-quântica;
- Levantar um quadro comparativo entre os principais algoritmos de criptografia pós-quântica;
- Selecionar alguns algoritmos de criptografia pós-quântica e demonstrar sua aplicabilidade com protocolos de comunicação já adotados atualmente;
- Realizar uma análise crítica sobre o status da computação quântica

Obrigado!