GERCOM

Quantum-Safe Cryptography

A Proteção da Informação na Era dos Computadores Quânticos

GERCOM

Tópicos

Introdução

- Os computadores quânticos representam uma ameaça aos sistemas criptográficos atuais.
- Algoritmos quânticos como Shor e Grover podem quebrar a criptografia tradicional.
- A criptografia precisa evoluir para resistir a ataques quânticos.

Complexidade Computacional e Criptografia

- **A criptografia se baseia em problemas matemáticos difíceis.**
  - **Fatoração de Números Inteiros**
  - **Logaritmo Discreto**
  - **Logaritmo Discreto em Curvas Elípticas**

Complexidade Computacional e Criptografia

- **Classe NP: Problemas cuja solução pode ser verificada rapidamente.**
- **NP-intermediário: Problemas como fatoração e logaritmo discreto.**
- **NP-completo / NP-hard: Usados na criptografia pós-quântica.**

ALGORITMOS

Impacto dos Computadores Quânticos

Shor's Algorithm

resolve fatoração e logaritmos discretos em tempo polinomial.

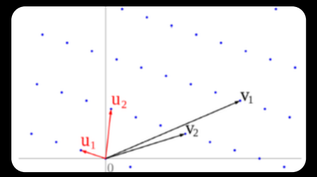
Grover's Algorithm

reduz segurança de algoritmos simétricos e funções hash.

Protocolos como RSA e ECC

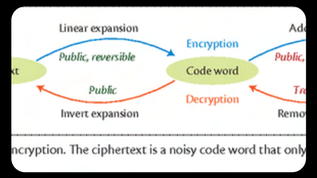
- precisam ser substituídos por algoritmos quantum-safe.

Tipos de Problemas para Criptografia Pós-Quântica



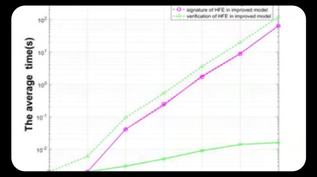
Lattice-based

Redes matemáticas complexas



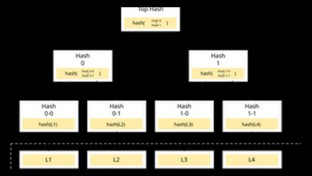
Code-based

Dificuldade em decodificação de códigos



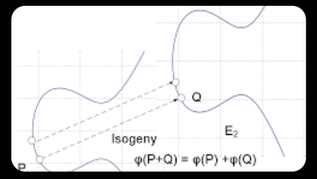
Multivariate

Equações polinomiais multivariadas



Hash-based

Assinaturas digitais baseadas em hash

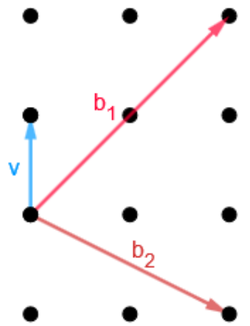


Isogeny-based

Baseado em curvas elípticas supersingulares

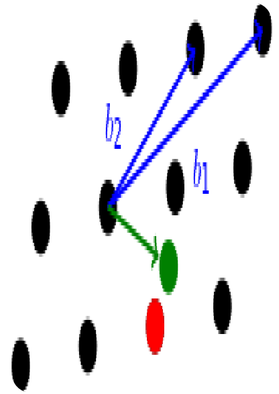
Lattice-Based Cryptography

Baseada na dificuldade de problemas em redes matemáticas.



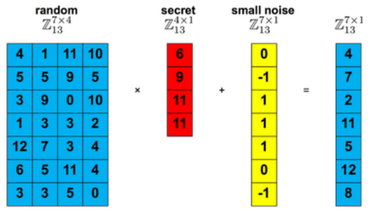
Shortest Vector Problem

Encontrar o vetor mais curto em um lattice.



Closest Vector Problem

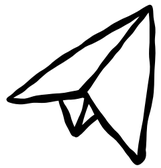
Encontrar o ponto do lattice mais próximo de um vetor externo.



Learning With Errors

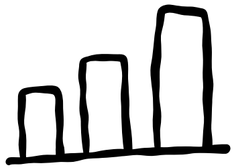
Problema de aprendizado com ruído, usado na construção de esquemas criptográficos.

Por que o SPHINCS+ foi escolhido?



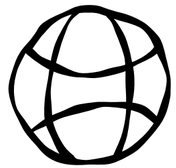
HASH

Baseado em funções hash, diferente dos demais candidatos lattice-based



BACKUP

Escolhido como opção de backup, garantindo diversidade matemática



RESISTÊNCIA EXTRA

Tem assinaturas maiores, mas oferece resistência extra a ataques futuros

Voltar à página de tópicos

Padronização do NIST

Desde 2016, o NIST conduz esforços para padronizar a criptografia pós-quântica

	CRYSTALS-Kyber	CRYSTALS-Dilithium	FALCON	SPHINCS+
TIPO	**Lattice-based**	**Lattice-based**	**Lattice-based**	**Hash-based**
FAZ o que?	**Encapsulamento de chaves.**	**Assinaturas digitais**	**Assinaturas digitais leves**	**Assinaturas digitais como alternativa segura**

CONCLUSÃO

Computadores quânticos ameaçam sistemas criptográficos clássicos.

A criptografia pós-quântica se baseia em problemas difíceis, como redes e códigos.

O NIST selecionou algoritmos promissores para garantir segurança futura.

A adoção desses padrões será essencial para proteger dados no longo prazo.
