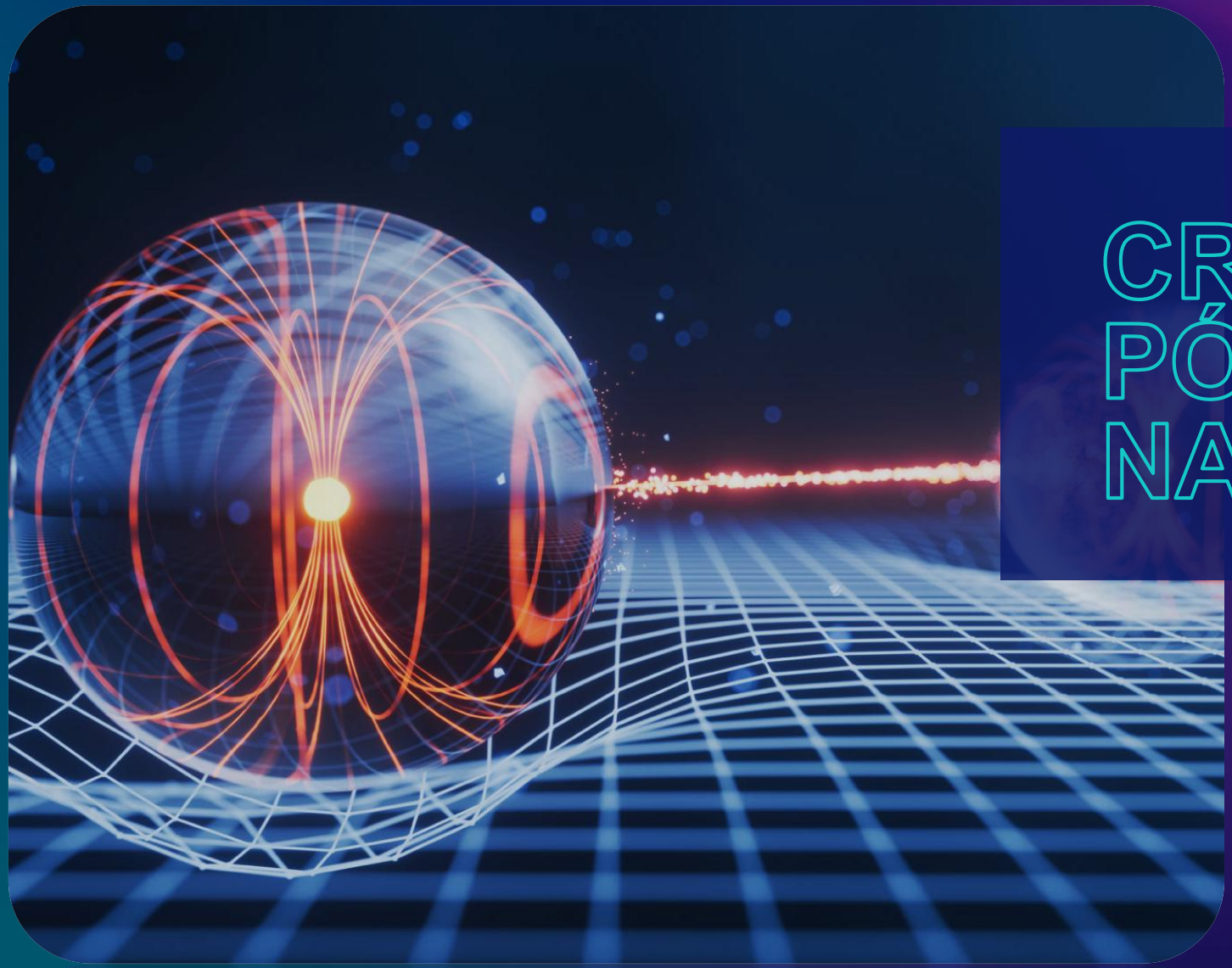

CRIPTOGRAFIA PÓS-QUÂNTICA NA NUVEM

Guilherme,
Gustavo,
Horácio,
João Victor

COMPUTAÇÃO QUÂNTICA

- Computação quântica é um campo multidisciplinar que compreende aspectos da ciência da computação, da física e da matemática e que utiliza a mecânica quântica para resolver problemas complexos mais rapidamente do que em computadores tradicionais.

- Os computadores quânticos são capazes de resolver certos tipos de problemas mais rapidamente do que os computadores tradicionais, aproveitando os efeitos da mecânica quântica, como superposição e interferência quântica. Algumas aplicações em que os computadores quânticos podem fornecer esse aumento de velocidade incluem machine learning (ML), otimização e simulação de sistemas físicos.

O QUE É UM BIT QUÂNTICO?

- Bits quânticos, ou qubits, são representados por partículas quânticas.
- A manipulação de bits quânticos por dispositivos de controle é a essência da capacidade de processamento de um computador quântico.
- Em sua essência, o processador de uma máquina tradicional realiza todo o seu trabalho ao manipular bits. De forma semelhante, o processador quântico realiza todo o seu trabalho ao processar bits quântico
- Na computação clássica, o bit corresponde a um sinal eletrônico que está positivo ou negativo. O valor do bit clássico pode ser um (positivo) ou zero (negativo). No entanto, como o bit quântico é baseado nas leis da mecânica quântica, ele pode ser colocado em uma superposição de estados (0 ou 1).

COMO A COMPUTAÇÃO QUÂNTICA AMEAÇA A CRIPTOGRAFIA ATUAL?

- A criptografia tradicional depende de algoritmos criptográficos – ou seja, equações matemáticas que precisam ser resolvidas para acessar os dados que estão protegendo.

- Três dos algoritmos mais usados atualmente – RSA, criptografia de curva elíptica e troca de chaves Diffie-Hellman – se baseiam no fato de que certos tipos de problemas matemáticos são extremamente difíceis de resolver com um computador clássico.

- Com a tecnologia atual, quebrar o padrão RSA mais avançado poderia levar bilhões de anos. No entanto, com um computador quântico, seria possível quebrar esses três esquemas criptográficos em apenas algumas horas.

COMO A COMPUTAÇÃO QUÂNTICA AMEAÇA A CRIPTOGRAFIA ATUAL?

- Estima-se que 90% das conexões na internet começam usando RSA para estabelecer uma comunicação segura, o que torna essa ameaça extremamente abrangente.

- Os computadores quânticos de hoje ainda não são capazes de quebrar a criptografia atual. Mas, de acordo com o mais recente Relatório de Cronograma de Ameaça Quântica do Global Risk Institute, “não há uma barreira fundamental conhecida para a realização da computação quântica em grande escala”.

- O relatório estima que há uma chance entre 17% e 31% de que, dentro de uma década, seja desenvolvido um Computador Quântico capaz de quebrar a criptografia RSA em menos de 24 horas – e uma chance entre 33% e 54% de que isso aconteça dentro de 15 anos.

SOLUÇÕES NA COMPUTAÇÃO EM NUVEM

- **Serviços de Gestão de Chaves (KMS):** Provedores que integram esquemas PQC nas suas bibliotecas (AWS-LC, SymCrypt) para que APIs e UIs de KMS possam gerar, armazenar e usar chaves pós-quânticas. Permite ao cliente ativar “quantum-safe” para operações de criptografia em repouso e em trânsito.

- **Compliance e Padrões:** Seguir os algoritmos padronizados pelo NIST (Kyber, Dilithium, SPHINCS+) e certificações FIPS garante interoperabilidade e conformidade regulatória na nuvem.

SOLUÇÕES NA COMPUTAÇÃO EM NUVEM

- **Handshakes Híbridos TLS:** Combina um algoritmo clássico (p.ex. ECDH) com um pós-quântico (p.ex. Kyber).Garante compatibilidade com clientes legados e adiciona resistência quântica ao transporte de dados em nuvem.

APLICAÇÃO DA CRIPTOGRAFIA PÓS-QUÂNTICA NA NUVEM

- **AWS Key Management Service (KMS),** ACM e Secrets ManagerAWS adicionou suporte a TLS híbrido pós-quântico (combina ECDH clássico e ML-KEM/Kyber) nos endpoints do KMS, ACM e Secrets Manager. Essa opção pode ser habilitada em conexões API para proteger dados em trânsito com um overhead de latência mínimo (≈ 80–150 µs) e cerca de 1 600 bytes extras no handshake

APLICAÇÃO DA CRIPTOGRAFIA PÓS-QUÂNTICA NA NUVEM

- **Google Cloud Key Management Service (Cloud KMS):** Em preview, o Cloud KMS já oferece:
- PQC para assinatura: algoritmos padronizados pelo NIST (PQ_SIGN_ML_DSA_65, PQ_SIGN_SLH_DSA_SHA2_128S) para criar e validar assinaturas digitais resistentes a computadores quânticos.
- Visão estratégica: roadmap para estender PQC a HSMs e demais produtos de criptografia na nuvem

APLICAÇÃO DA CRIPTOGRAFIA PÓS-QUÂNTICA NA NUVEM

- **IBM Cloud Key Protect:** Permite conexões TLS “quantum-safe” em dois modos: puro (só Kyber) e híbrido (ECDH + Kyber), com endpoints dedicados em regiões como US-South (qsc.us-south.kms.cloud.ibm.com) e EU-GB (qsc.eu-gb.kms.cloud.ibm.com).

- Essa proteção cobre apenas o tráfego em trânsito, enquanto o armazenamento em repouso continua com AES-256, que já oferece segurança quântica forte (~128 bits).

APLICAÇÃO DA CRIPTOGRAFIA PÓS-QUÂNTICA NA NUVEM

- **Cloudflare (CDN e borda):** Desde outubro de 2022, todas as conexões TLS 1.3 via Cloudflare suportam acordos de chave híbridos pós-quânticos (ex.: X25519MLKEM768), garantindo proteção contra o ataque “store-now, decrypt-later” mesmo antes da adoção generalizada pelos navegadores cliente.

DESAFIOS E TENDÊNCIAS FUTURAS

VULNERABILIDADE DE DADOS

Os hackers estão armazenando dados criptografados hoje para descriptografar por computadores quânticos no futuro, ameaçando os dados confidenciais das organizações no longo prazo.

PADRÕES, PRESSÃO E INCERTEZA

As organizações devem adotar rapidamente soluções cripto ágeis para cumprir os prazos de segurança quântica 2030-2035 do NIST enquanto navegam por padrões e desafios técnicos em evolução.

BARREIRAS DE IMPLEMENTAÇÃO

A integração da criptografia pós-quântica (PQC) na infraestrutura existente apresenta obstáculos técnicos, incluindo compatibilidade legada, impactos no desempenho e prazos de conformidade.