

JÁ NÃO É FICÇÃO

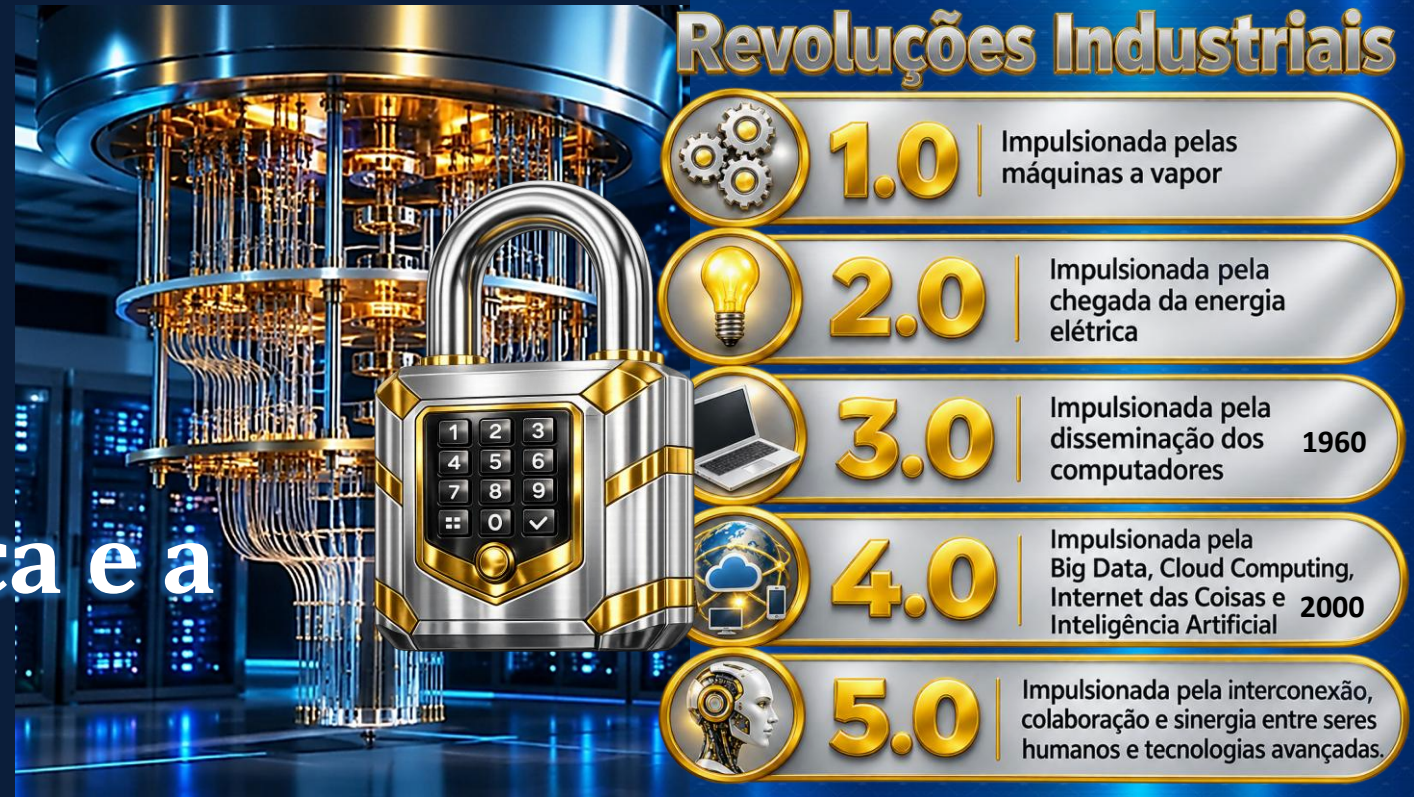
Dia 2 de 3

A Ameaça Criptográfica e a Convergência com a Indústria 5.0

Já vimos que o presente da supercomputação é híbrido. Hoje veremos o lado sombrio da mesma moeda e seus impactos em IoT e na Indústria.

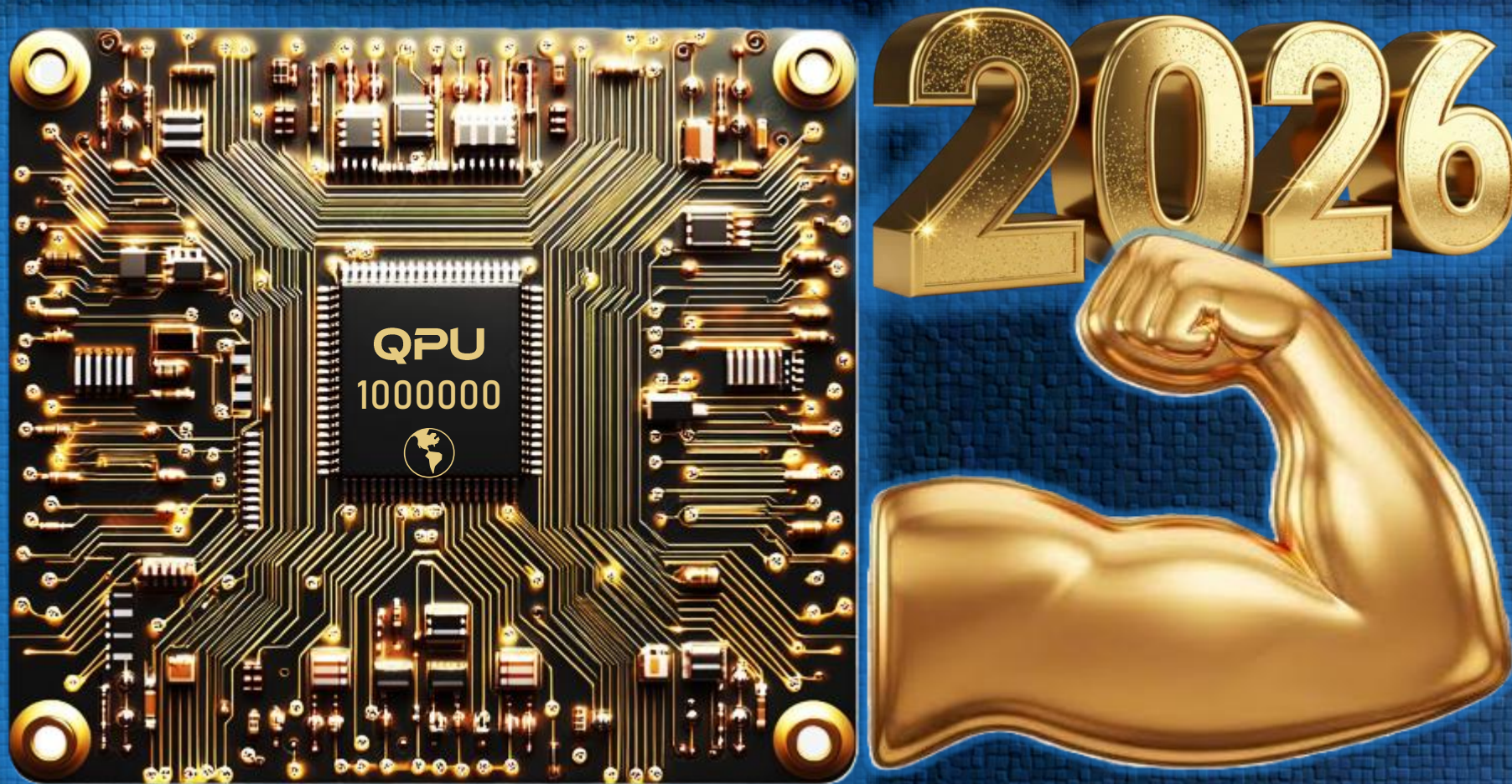
João Roberto Peres

Dia 2 — Já não é ficção — 29/09/2026



FÓRUM
BRASILEIRO
DE IoT

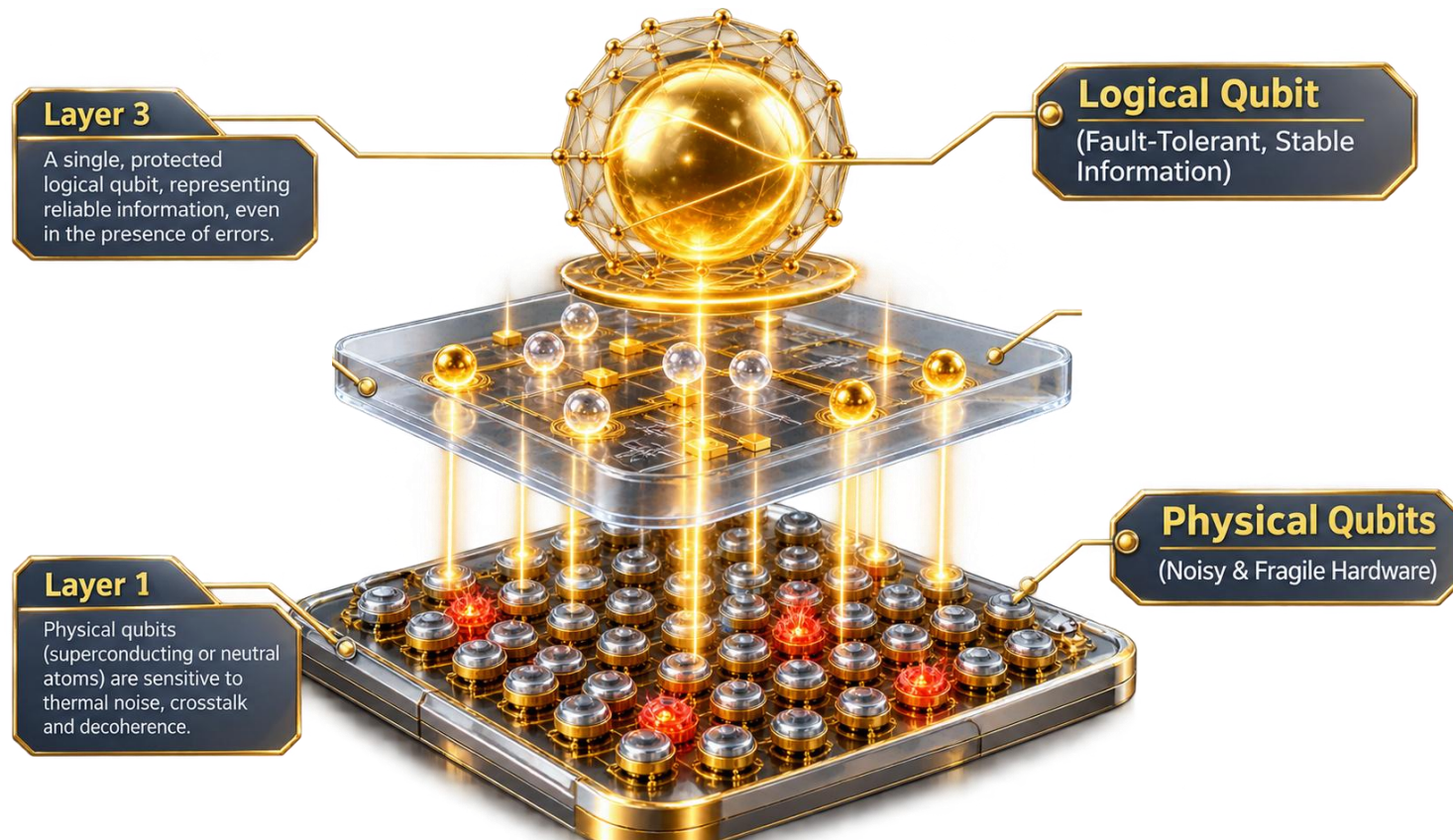
Poder Computacional Quântico



A SEGUIR: INFORMAÇÕES ALTAMENTE DIDÁTICAS – NÃO BUSCAM PRECISÃO CIENTÍFICA E TECNOLÓGICA.

O Fundamento – QuBits – Físicos e Lógicos.

Da fragilidade dos qubits físicos à robustez dos qubits lógicos



QEC não elimina o erro: ela torna o erro detectável, tratável e, em condições suficientemente para viabilizar a computação quântica tolerante a falhas.

O desafio: qubits físicos são frágeis.

- Ruído, decoerência e erros de operação afetam continuamente os qubits físicos.
- Um qubit físico isolado não oferece a confiabilidade necessária para computação quântica de longa duração.
- A escalabilidade exige uma forma de detectar e tratar erros sem destruir a informação quântica.

A resposta: Quantum Error Correction (**QEC**)

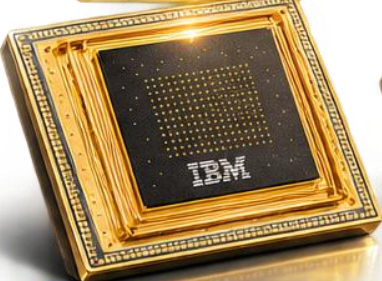
- Vários qubits físicos + qubits ancilla (auxiliar) são combinados para codificar um qubit lógico.
- A Nondemolition Measurement (medição de síndromes de erro) revela onde e qual tipo de erro ocorreu, sem medir diretamente o estado lógico.
- Um decodificador (QEC Decoder) interpreta essas informações e orienta a correção, reduzindo a taxa efetiva de erro.
- **QEC** é a ponte de hoje, entre hardware quântico ruidoso e computação quântica tolerante a falhas útil.

O Fundamento – Qubits X Poder Computacional



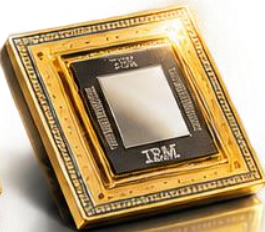
O PODER COMPUTACIONAL NÃO DEPENDE DA QUANTIDADE DE QUBITS FÍSICOS

IBM Condor
1.121 qubits



Mais qubits físicos,
mas alta taxa de erro.

IBM Heron
133 qubits



Menos qubits,
mais fidelidade.

1. Desempenho

- O Condor tem desempenho comparável a chips muito menores (ex.: Osprey – 433 qubits).

2. Taxa de erro e ruído

- Arquitetura Heavy-Hexagonal de frequência fixa.
- Crosstalk e ruído quântico continuam altos.
- Não executa circuitos longos ou complexos.

3. Condor vs. Heron

- O Heron (133 qubits) reduz drasticamente os erros e entrega 3 a 5x mais desempenho.
- O Condor sacrificou a qualidade em prol do tamanho.

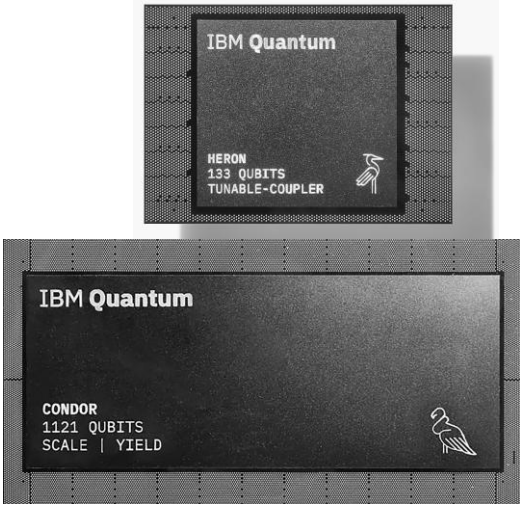
Comparação de Abordagens (IBM Summit)		
Métrica / Chip	IBM Condor	IBM Heron
Qubits Físicos	1.121	133
Foco de Engenharia	Escalar tamanho e cabeamento criogênico	Redução extrema de erros quânticos
Poder Real Prático	Baixo (sofre com alta interferência)	Alto (executa cálculos mais profundos)
Utilidade	Banco de testes para correção de erros	Computação quântica de utilidade real

Para que serve o Condor?

- Laboratório de engenharia física.
- Testa códigos de correção de erros quânticos.
- Prova a capacidade da IBM de construir sistemas gigantesco.
- Plataforma para o futuro da computação quântica de utilidade real.

Tecnologias qubits supercondutores exigem criogenia.

O verdadeiro poder computacional vem da **qualidade dos qubits** (fidelidade), não apenas da sua quantidade.



Hoje o poder computacional depende da tecnologia do chip, tipo de QPU e do sistema de verificação de erros “Nondemolition Measurement” (medição de síndromes de erro) e correção através do Quantum Error Correction (QEC).

Como se viabiliza a Computação Quântica?

RMN: uma plataforma compacta para processamento

Como funciona (visão didática):

- Campo magnético + RF e amplificares controlam os spins nucleares.
- A base líquida de 10 ml* do magneto processador contém **moléculas com spins nucleares**.
- A sonda de RMN excita o liquido do recipiente de 10 ml na base de processamento e detecta os sinais.
- A eletrônica realiza controle, processamento e leitura do processamento realizado por molécula (qubit-físico).
- Esta tecnologia também usa o Decodificador QEC (QEC Decoder).

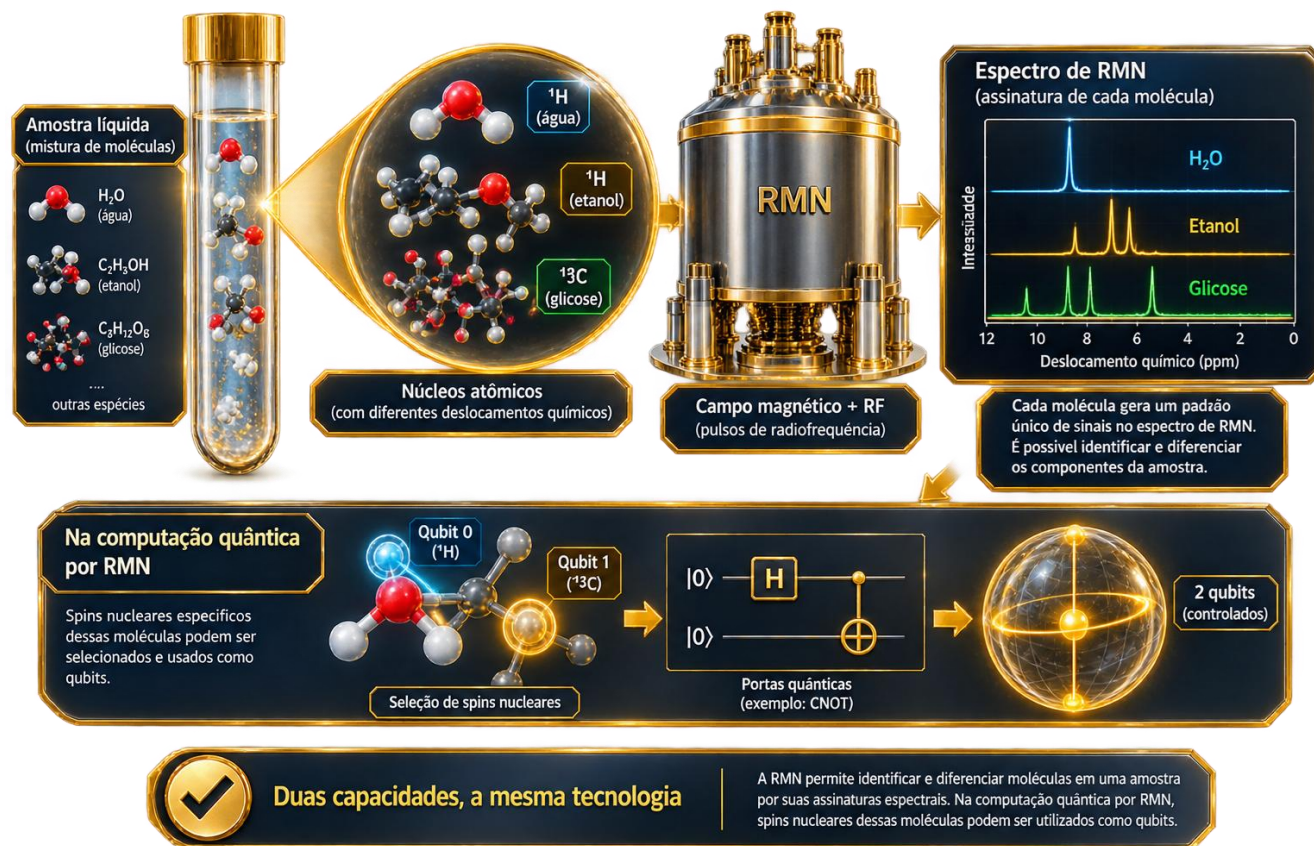
*Apenas como curiosidade: – a solução (H₂O + etanol+glicose) em 10 ml tem aproximadamente acentenas de sextilhões de qubits físicos (10²³) devido às propriedades químicas dos componentes.

Componente	Quantidade na Mistura	Mols Estimados	Número de Moléculas
Água	8,0 ml (~8,0 g)	0,444 mol	~ 2, 67 × 10 ²³
Etanol	1,5 ml (~1,18 g)	0,026 mol	~ 0, 16 × 10 ²³
Glicose	0,5 g	0,003 mol	~ 0, 02 × 10 ²³
Total Estimado	10 ml	0,473 mol	~ 2, 85 × 10 ²³ moléculas



RMN: da Identificação Molecular à Computação Quântica.

RMN: Computação Quântica Qubits



RMN como ferramenta analítica:

- Identifica e diferencia moléculas por suas assinaturas espectrais.
- Deslocamentos químicos, acoplamentos e intensidade dos sinais revelam a composição molecular.
- Uma mesma amostra de 10 ml na área de processamento pode conter diferentes moléculas e produzir padrões espectrais distintos. No caso água + etanol + glicose.

RMN como plataforma quântica:

- Spins nucleares selecionados atuam como qubits.
- Pulsos de radiofrequência implementam operações e portas quânticas.
- Spins controlados permitem demonstrar processamento em qubits, incluindo portas como a CNOT e outras funcionalidades.

A mesma física dos spins nucleares pode servir tanto para identificar moléculas quanto para realizar processamento quântico.

Na realidade as máquinas da SpinQ Technology utilizam os spins dos núcleos atômicos de moléculas líquidas (como o **trifluoroetileno** (C_2HF_3)) aprisionadas dentro de um pequeno frasco selado.

$\sim 2,85 \times 10^{23}$ (10 elevado a 23ª) é igual a 1 seguido de 23 zeros (100.000.000.000.000.000.000.000), que equivale a 100 sextilhões. Cem sextilhões (no padrão brasileiro/escala curta).

Um testemunho de 28/09/2026



Do Anúncio no Workshop à Realidade na Prática

Neste workshop do Fórum Brasileiro de IoT (24/09), o nosso convidado **Yanis Stoyannis** (Customer Security Director na Ericsson) revelou que iria visitar a infraestrutura quântica do SENAI SP.

Em 28/09, Yanis cumpriu a visita em São Caetano do Sul e compartilhou o registo fotográfico: um testemunho direto do **SpinQ Triangulum** — a primeira plataforma quântica do Brasil adquirida para treino industrial (modelo 2022, entregue em 2023) —, atualmente operacional e ligada em rede LAN.

Yanis Stoyannis  · 1º

Customer Security Director | ERICSSON. Cyber Security Strategist to better protect an Interconnected World. MBA in Cyber Security Professor, Speaker, Writer.

<https://www.linkedin.com/in/yanis-stoyannis/>

Computação Quântica precisa de RAM e SSD?

O papel da memória clássica e da memória quântica.



A computação quântica atual não elimina a memória clássica: ela acrescenta uma nova camada de processamento quântico a uma arquitetura predominantemente híbrida.

Onde está a memória hoje?

- RAM e SSD continuam sendo componentes clássicos da arquitetura de um sistema quântico.
- O SSD armazena programas, dados, parâmetros, circuitos quânticos e resultados.
- A RAM mantém dados e instruções durante o processamento e a comunicação com a QPU.
- CPU/GPU/NPU + QPU trabalham de forma híbrida em muitas arquiteturas atuais.

E a “memória quântica”?

- Quantum Memory armazena estados quânticos preservando suas propriedades quânticas por determinado período.
- Pode utilizar átomos, íons, spins, fótons ou outros sistemas quânticos, dependendo da tecnologia – existem diversas marcas comerciais: – (Welinq – Qdrive), (IonQ + Lightsynq), (Photon Queue), (cryo-CMOS SRAM).
- É particularmente relevante para redes quânticas, repetidores quânticos e comunicação quântica.
- Ainda não existe uma substituição direta da RAM/SSD por memória quântica de uso geral.

O impacto do Poder Computacional Quântico Hoje



O Algoritmo Que Muda Tudo – quebra a atual criptografia mundial

O Algoritmo de “Shor” para computadores eletrônicos quânticos



Hoje: RSA e ECC

Protegem transações bancárias, assinaturas digitais e o tráfego HTTPS, baseados em problemas matemáticos que um computador clássico levaria milhares de anos para reverter.

RSA = Ron Rivest, Adi Shamir e Leonard Adleman, os criadores do algoritmo em 1977.
ECC = Elliptic Curve Cryptography – algoritmo criado em 1985.



Com uma QPU madura

O Algoritmo de Peter Shor (1994) resolve a chave cripto em tempo polinomial, derivando a chave privada a partir da pública em questão de minutos. Ou seja, quebra a segurança. Hoje QCs levam meses, só não sabemos quantos meses, dias, horas, ou minutos – depende da capacidade.

O risco já existe - “Colha agora, decifre depois”

O Harvest Now, Decrypt Later (**HNDL**) não depende de um computador quântico capaz de quebrar a criptografia hoje. Dados criptografados podem ser capturados e armazenados atualmente, para eventual decifração futura por computadores capazes de comprometer os algoritmos utilizados.

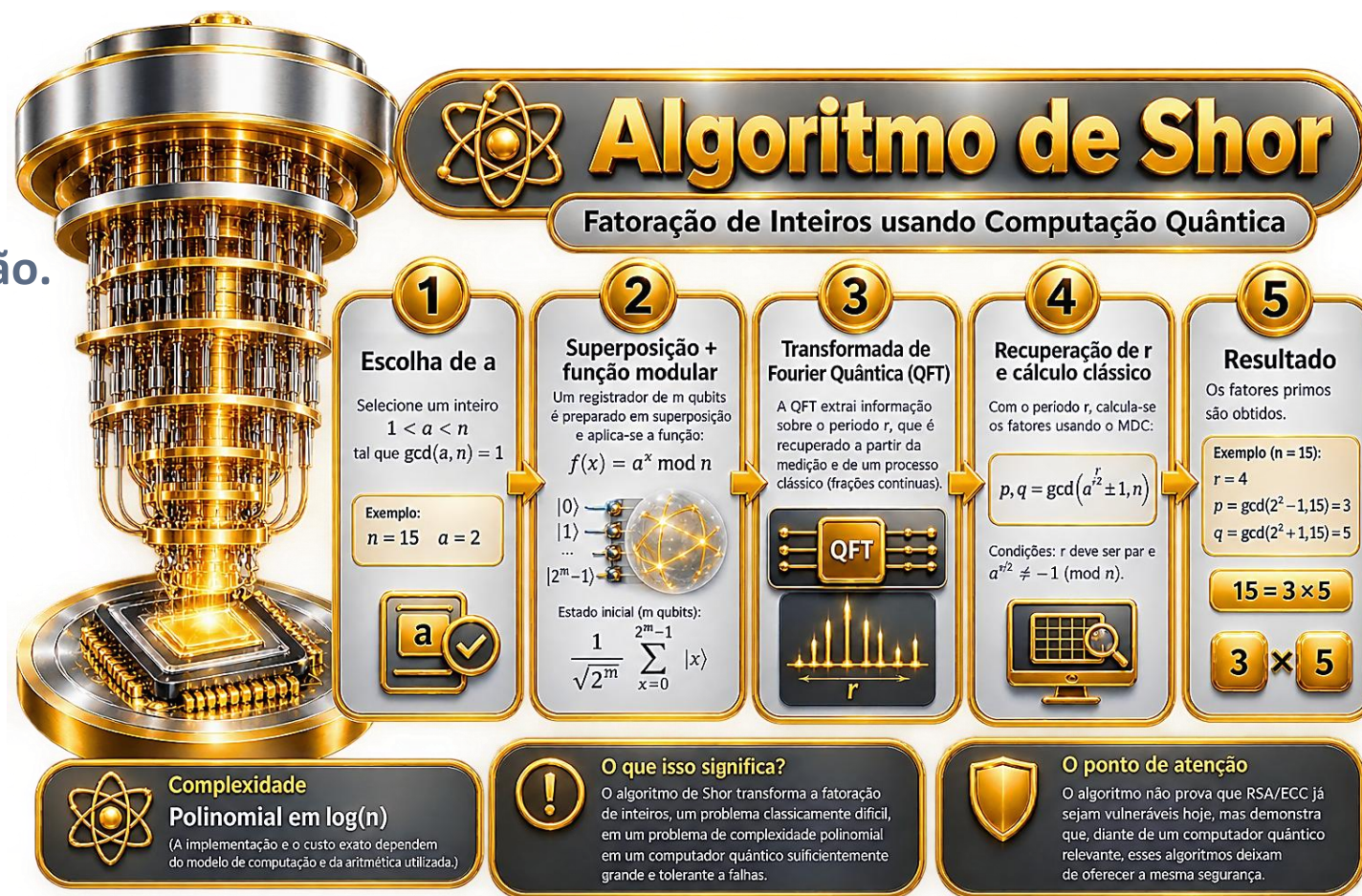
O Algoritmo Shor

A Ameaça à Criptografia Atual

Algoritmo de Shor/Grover – o risco com solução.

- **Criptografia atual:** sistemas como RSA dependem da dificuldade de fatorar números gigantes com computadores clássicos.
- **O atalho quântico:** o Algoritmo de Shor permite, em princípio, que um computador quântico suficientemente potente fatore esses números de forma exponencialmente mais eficiente em poucos minutos.
- **Impacto prático:** com hardware quântico escalável e tolerante a falhas, a criptografia de chave pública atualmente utilizada poderá se tornar vulnerável, comprometendo dados confidenciais e comunicações protegidas.

<https://www.fortinet.com/br/resources/cyberglossary/shors-grovers-algorithms>
<https://quantum.microsoft.com/en-us/insights/education/concepts/quantum-algorithms>
<https://proceedings.sbm.org.br/sbm/article/view/5101>
https://pennylane.ai/demos/tutorial_grovers_algorithm



Infográfico ilustrativo - versão simplificada – sem objetivo de demonstração matemática.

O NIST (Instituto Nacional de Padrões e Tecnologia dos EUA) lançou oficialmente o seu primeiro conjunto de padrões da família de algoritmos de Criptografia Pós-Quântica (PQC) para proteção - em 13 de agosto de 2024.

Alerta Nacional

A Visão da ABIN sobre a Ameaça Quântica

- **Prioridade de Segurança Nacional:** O relatório Desafios de Inteligência (2026) da ABIN classifica a transição pós-quântica como questão de sobrevivência e soberania de dados para o Estado.
- **O Risco do "Apocalipse Quântico":** Cenário em que atacantes conquistam capacidade quântica antes da migração, exigindo planos extremos de contingência, corte de comunicações e revogação em massa de materiais criptográficos.
- **Mobilização do Estado:** A inteligência brasileira já atua na atualização de infraestruturas de Chaves Públicas, criptografia estatal e armazenamento seguro de dados em clouds governamentais (SERPRO).
- **Urgência Executiva:** Se a Segurança de Estado e as infraestruturas críticas do governo já estão movendo suas peças, o setor privado precisa inventariar seus ativos e iniciar a migração PQC para garantir resiliência antes que seja tarde.

Transição pós-quântica na Inteligência de Estado

Para a Inteligência de Estado, a transição pós-quântica não é um tema apenas técnico, mas um problema de prioridade nacional que redefine o ciclo de vida da informação sigilosa. A Inteligência trabalha com horizontes de sigilo que atravessam governos, por isso, o risco do ataque "coletar agora, decifrar depois" é estrutural para fontes e métodos. Uma eventual quebra retroativa de dados sigilosos pode expor identidades, rotinas e técnicas.

Para a Inteligência, destacam-se dois cenários. No primeiro, o Estado provê resposta preventiva, em que a transição pós-quântica é executada antes de um computador quântico com alto poder computacional estar disponível. Essa resposta começa por uma triagem completa dos acervos e dos canais a serem protegidos, priorizando conteúdos pelo valor informacional e pela vida útil do sigilo. Adotam-se protocolos híbridos (os quais combinam algoritmos clássicos e pós-quânticos), define-se ritmo de rotação de chaves e estabelecem-se critérios de revalidação e re-assinatura com carimbo do tempo confiável, preservando a cadeia de custódia e a compatibilidade entre sistemas.

No segundo cenário, conhecido como "apocalipse quântico", o adversário conquista capacidades quânticas antes de a transição pós-quântica ter sido finalizada. Nesse cenário, o atacante poderá ter acesso a dados sigilosos. O plano de contingência deve prever corte rápido da comunicação, revogação e reemissão de materiais criptográficos, isolamento e compartimentalização de redes e acervos sensíveis, além de reestabelecimento das âncoras de confiança (*re-trust*) e re-assinatu-

**DESAFIOS DE
INTELIGÊNCIA**
EDIÇÃO 2026



Avaliação do Risco Criptográfico Quântico

Impacto Severo Constante

- **Impacto Inegociável (Sempre Alto):** A eventual quebra dos algoritmos de chave pública (RSA / ECC) compromete a confidencialidade, autenticidade e assinaturas digitais.
- **Curva de Probabilidade Crescente:** À medida que a tecnologia de hardware quântico amadurece, a probabilidade de um ataque viável migra de baixa para iminente.
- **Ausência de "Risco Baixo":** Mesmo no cenário imediato, o risco mínimo apurado é Médio, justificando a urgência na preparação.
- **Janela Crítica de Ação:** O tempo necessário para inventariar, homologar e substituir sistemas criptográficos em escala exige iniciar a migração PQC antes que o risco atinja o nível extremo.



Na corrida geopolítica por Chips, IA e Computação Quântica, o *Q-Day* não terá aviso prévio — quem liderar essa hegemonia chegará em silêncio"



Pesquisa Imediata com IAG

Desafio Rápido: Faça dois testes na sua IA preferida agora mesmo:

Pergunta 1: "Computadores quânticos hoje conseguem quebrar o RSA?"

Resposta da IA: NÃO.

Pergunta 2: "Se um Governo ou Agência de Inteligência conseguisse quebrar o RSA hoje, ele avisaria o mundo em público?"

Resposta da IA: NÃO.

A minha provocação: Você e a sua organização esperaria um anúncio oficial que nunca acontecerá para começar a se proteger?

O Q-Day Chegou Mais Perto

A revisão do Caltech encurtou o horizonte de risco



Milhões

de qubits físicos era a estimativa antiga para um computador tolerante a falhas capaz de rodar o Shor



~10 mil

qubits físicos, segundo os novos códigos de correção de erro de alta taxa do Caltech (Instituto de Tecnologia da Califórnia -2024)



<https://tek.sapo.pt/noticias/computadores/artigos/o-q-day-esta-mais-perto-do-que-esperavamos-alertas-sobem-de-tom-com-os-avancos-na-computacao-quantica/>
<https://www.gizmodo.com.br/o-q-day-pode-desencadear-a-maior-crise-de-ciberseguranca-da-historia-e-gigantes-da-tecnologia-acreditam-que-ele-esta-muito-mais-proximo-do-que-imaginavamos-53975>
<https://www.scrippsnews.com/scripps-news-investigates/q-day-americas-quantum-computing-blindspot/the-coming-q-day-us-states-largely-unprepared-as-quantum-computing-threats-loom>
<https://thequantuminsider.com/2026/03/31/q-day-just-got-closer-three-papers-in-three-months-are-rewriting-the-quantum-threat-timeline/>
<https://www.qusecure.com/google-accelerates-q-day-migration-timeline-to-2029/> 09 de abril de 2026

Quem está Mais Exposto



Setor Financeiro

Os certificados e assinaturas digitais podem ser comprometidas inclusive afetar o PIX.

Open Finance, pagamentos instantâneos e assinaturas digitais entre outros dependem de ECC e RSA para o não repúdio de transações e contratos.

<https://www.broadcast.com.br/news/voce-ja-ouviu-falar-em-computacao-quantica-seu-banco-ja/>
<https://www.cnnbrasil.com.br/branded-content/nacional/na-vanguarda-da-inovacao-bradesco-se-prepara-para-a-era-da-computacao-quantica/>

Situação Atual no Brasil

Os principais bancos no Brasil já iniciaram os preparativos para a transição para a Criptografia Pós-Quântica (PQC), antecipando-se aos riscos que a computação quântica poderá trazer aos sistemas de segurança digital.

Alguns casos:

- **Bradesco:** Iniciou em 2023 o programa **QSAFE**, voltado para testes com algoritmos pós-quânticos e adoção controlada em sistemas de maior exposição.
- **Itaú:** Estruturou pesquisas sobre **agilidade criptográfica** e segurança por meio do Instituto de Ciência e Tecnologia Itaú (ICTi), expandindo iniciativas iniciadas no final da década passada.
- **Banco Central (BC):** O órgão regulador já discute a criação de um **arcabouço normativo** para mitigar riscos tecnológicos futuros, debatendo o tema em eventos como o Febraban Tech.
- **A Federação Brasileira de Bancos (Febraban)** atua como o principal orquestrador setorial e fórum de padronização para a **transição PQC** no Brasil. A entidade entende que a segurança quântica não é um diferencial competitivo para marcas individuais, mas sim uma exigência de resiliência sistêmica para proteger toda a infraestrutura financeira nacional.

Quem está Mais Exposto

Gargalos Críticos de Exposição Quântica

- **Dispositivos implantados hoje:** estarão ativos quando o Q-Day chegar, tornando a falta de atualização (crypto-agility) um risco imediato.
- **Ataque Harvest Now, Decrypt Later:** Dados sensíveis de saúde, segredos industriais e comunicações de Estado interceptados hoje estão sendo armazenados para decodificação futura por computadores quânticos.
- **Sistemas Legados sem Suporte:** Infraestruturas bancárias, industriais e de telecomunicações rodando em hardwares antigos que não possuem memória ou capacidade de processamento para rodar os novos algoritmos PQC -Lightweight .
- **Dependência da Criptografia de Chave Pública:** Qualquer arquitetura baseada nos padrões atuais (RSA, ECC e certificados digitais ICP) perderá a capacidade de garantir autenticidade, integridade e não-repúdio.



IoT de Ciclo de Vida Longo

Sensores industriais e medidores inteligentes operam 15 a 25 anos, sem capacidade de atualização remota de criptografia (*crypto-agility*).

Grande impacto na Indústria.

<https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2025/02/Post-Quantum-Cryptography-in-IoT-Ecosystem-1.pdf>
<https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/post-quantum-cryptography-in-iot/>
<https://sol.sbc.org.br/index.php/sbrc/article/view/42308>

Quem Está Mais Exposto



Setor Jurídico

As assinaturas digitais podem ser comprometidas.

Ameaça ao sigilo profissional.

Vulnerabilidades de Contratos.

Proteção e privacidade de dados de clientes.

<https://oabdf.org.br/criptografia-pos-quantica-e-desafios-da-ciberseguranca-entram-em-debate-na-oab-df/> (31/10/2025)

<https://peckadv.com.br/criptografia-hoje-violacao-amanha-a-problematiza-do-harvest-now-decrypt-later-frente-aos-limites-do-direito-penal-e-da-regulacao-de-incidentes-no-brasil/>

<https://www.migalhas.com.br/quentes/459145/governo-se-prepara-para-a-era-quantica-diz-advogada>

<https://www.cnmp.mp.br/portal/todas-as-noticias/19498-cnmp-debate-os-desafios-da-seguranca-digital-e-da-protecao-de-dados-em-conferencia-sobre-ciberseguranca>

Falta de Preparo é Risco Crítico

A vulnerabilidade não decorre apenas de TI, mas da própria essência do exercício da advocacia e da responsabilidade civil dos escritórios:

Quebra do Sigilo Profissional (Art. 34 do EAOAB): O segredo do cliente é um dever legal. O risco Harvest Now, Decrypt Later significa que interceptações de e-mails, minutas corporativas, segredos industriais e estratégias de litígios trafegando hoje sem proteção pós-quântica poderão ser lidos no futuro.

Validade Jurídica de Contratos e Assinaturas Digitais: A infraestrutura de chaves públicas atual (ICP-Brasil) e os certificados digitais (A1/A3) usam algoritmos assimétricos (RSA/ECC) vulneráveis ao Algoritmo de Shor. Sem a transição para PQC, a irrefutabilidade e a autoria de contratos de longo prazo ficam expostas à contestação futura.

Responsabilidade Civil e LGPD (Art. 46): Escritórios de advocacia gerenciam volumes massivos de dados sensíveis. O descaso com a atualização dos padrões de criptografia diante de alertas de segurança nacional pode ser interpretado como negligência grave em deveres de mitigação de riscos ciberseguros.

Dependência do Judiciário e Prova Digital: Se os tribunais não atualizarem tempestivamente suas cadeias de custódia e infraestruturas do Processo Judicial Eletrônico (PJE), a integridade das provas digitais juntadas aos autos ficará juridicamente comprometida.

A Resposta Principal: PQC

Criptografia Pós-Quântica: os três padrões do NIST

FIPS 203 (ML-KEM)	Troca segura de chaves em redes
FIPS 204 (ML-DSA)	Assinaturas digitais e autenticação
FIPS 205 (SLH-DSA)	Assinaturas baseadas em hash, alternativa conservadora 64/128



São algoritmos que rodam em hardware clássico já existente. Não é preciso esperar o computador quântico chegar para se proteger dele.

<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
<https://ancd.org.br/icp-brasil-inicia-planejamento-para-migracao-a-criptografia-pos-quantica/>
<https://stickybit.com.br/bacen-pqc-2028/>
<https://pqca.org/>



A Resposta Principal: PQC para IoT

Criptografia Pós-Quântica de Baixo Custo Computacional: os padrões e abordagens do NIST

Ascon — NIST SP 800-232	Criptografia leve: AEAD, hash e XOF para dispositivos com recursos restritos, incluindo IoT, sistemas embarcados e sensores de baixo consumo.
FN-DSA (Falcon)	Assinatura digital pós-quântica: algoritmo baseado em reticulados, com chaves públicas e assinaturas pequenas. É relevante quando IoT precisa de assinaturas PQC, mas não é o padrão LWC do NIST.
PQC híbrido + criptografia clássica	Estratégia de transição: combinação de mecanismos clássicos e PQC durante a migração. Pode aumentar custo computacional, memória e complexidade; sua adequação depende do dispositivo e da aplicação.

Veja atualizações recentes e procure por PQC for IoT: <https://csrc.nist.gov/Projects/post-quantum-cryptography/publications>

***São padrões desenhados para microcontroladores e sensores de recursos restritos.
Permitem proteger redes de IoT e infraestruturas críticas sem exigir a troca do hardware existente.***

A Resposta Complementar: QKD

Distribuição Quântica de Chaves: segurança pela física, não pela matemática



- Usa fótons individuais: qualquer interceptação perturba fisicamente o estado quântico e denuncia o invasor
- Exige fibra óptica dedicada ou enlace de satélite, com alcance e custo consideráveis
- Não substitui a PQC: protege só a etapa de troca de chave, não a autenticação completa



A própria NSA americana, em suas diretrizes CNSA 2.0, recomenda a PQC como caminho primário e **não aprova QKD** isolada para Sistemas de Segurança Nacional.

QKD fica reservada a enlaces de altíssimo valor, apesar de estar evoluindo em pesquisas.

<https://postquantum.com/cnsa-2-0/complete-guide/> (guia completo requisitos de migração)

<https://quantumsecuritydefence.com/insights/why-qkd-not-substitute-pqc-migration/>

<https://www.datacenterdynamics.com/br/not%C3%ADcias/novo-projeto-do-cpqd-tem-foco-no-uso-de-tecnologias-quanticas-para-a-seguranca-cibernetica/>

<https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>

A Ponte Quântica: Da Realidade 3.0/4.0 à Indústria 5.0 no Brasil

Os Pilares da Indústria 5.0: Hiperpersonalização, resiliência na cadeia de suprimentos, sustentabilidade e colaboração homem-máquina em tempo real, tudo apoiado por supercomputação.



A Realidade Brasil (3.0 / 4.0)

Foco: Conectividade, Sensores e Automação

Gargalo: Hardwares IoT com ciclo de vida longo (15–20 anos) operando em redes vulneráveis.

Risco: Modernizar a fábrica com padrões criptográficos que serão obsoletos em breve.



O Salto Quântico (Indústria 5.0)

Foco: Decisão em tempo real, Sustentabilidade e PQC.

Solução Quântica: Algoritmos de otimização de malha logística e Criptografia Pós-Quântica leve no firmware.

Estratégia: Inserir a **Crypto-Agility** (agilidade criptográfica) desde o planejamento da automação 4.0.



"A Indústria 4.0 automatizou o chão de fábrica e dispensou processos manuais. A Indústria 5.0 faz o oposto: ela exige o humano de volta para tomar decisões estratégicas e éticas ao lado da máquina. O desafio dos Conselhos não é apenas comprar tecnologia pós-quântica ou IA, mas capacitar as pessoas que vão operar esse ecossistema."

A Indústria 5.0



Resiliência quântica e Resiliência industrial são a mesma pauta em muitas indústrias hoje



Resiliência Operacional

Sistemas Ciber-físicos, Cobots e gêmeos digitais em rede exigem comunicação protegida contra HNDL



Sustentabilidade

Algoritmos variacionais (VQE*-Variational Quantum Eigensolver) simulam materiais e catalisadores mais limpos



Centralidade Humana

QML** filtra bilhões de dados de sensores, entregando cenários preditivos ao gestor

* <https://quantagram.org/articles/qaoa-and-vqe/> ** <https://www.quera.com/glossary/quantum-machine-learning>

<https://revolus.com.br/industria-5-0-no-brasil/>

A Quarta Frente: Sensoriamento Quântico

Além do processamento: medir com superprecisão é realidade hoje



- **Magnetômetros** de diamante sintético detectam microfissuras antes que virem falha catastrófica. (Fadiga Mecânica e Estrutural - Falhas em Semicondutores e Microchips...)
- **Relógios atômicos** de escala de chip sincronizam Smart Grids e redes 5G/6G com precisão inédita.
- **Tipos de Sensores Quânticos:** Interferômetros atômicos, Magnetômetros de centros NV em diamante, Magnetômetros de vapor atômico, Dispositivos Supercondutores de Interferência Quântica (SQUIDS), Giroscópios de spin nuclear, Relógios atômicos de rede óptica, Sensores de Rydberg, Detectores de fóton único (SNSPDs), Sensores baseados em estados emaranhados e comprimidos (squeezed light), Gravímetros de átomos frios. ...

O sensoriamento não compete com o processamento, ele o alimenta . É por isso que a era quântica atua como uma infraestrutura híbrida silenciosa por trás da manufatura avançada, e não como um capítulo isolado de ficção corporativa.

Internet das Coisas Quânticas" (QIoT).

A sinergia resolve os principais gargalos da IoT atual



- A convergência entre sensores quânticos e a Internet das Coisas (IoT) representa o próximo grande salto tecnológico para indústrias, medicina e cidades inteligentes, criando a chamada "**Internet das Coisas Quânticas**" ou arquitetura (QIoT).
- Enquanto os sensores IoT tradicionais medem grandezas físicas de forma macroscópica, os sensores quânticos manipulam estados da matéria (como spins de elétrons ou átomos ultrafrios) para alcançar uma precisão até 1 milhão de vezes maior.
- A infraestrutura da QIoT (IEEE*) funciona como um sistema híbrido. Como sensores comuns na ponta (como termômetros ou câmeras de segurança) não possuem capacidade física de processamento quântico, a arquitetura é estruturada em camadas dinâmicas: **Camada de Percepção Quântica (Edge)**, **Camada de Transmissão Quântica**, **Camada de Controle e Processamento**.

Para que a IoT adote os sensores quânticos em larga escala, a indústria trabalha na miniaturização dos componentes. O objetivo atual é integrá-los em microchips de silício (chips fotônicos e eletrônicos integrados), permitindo que sejam instalados em pequenos dispositivos de borda (edge computing) e alimentados por baterias comuns de IoT.

* <https://ieeexplore.ieee.org/document/11014927> <https://nme.put.poznan.pl/quantum-internet-of-things-q-iot-physical-layer-precursors/>

Você pode validar e comprovar todas as informações fornecidas – todas elas são de fontes abertas que precisam ser mineiradas.



Pesquisa Interrogativa com Claude

*Use as técnicas de Engenharia de prompts SPIN/STAR/MDM-AI e outras para refinar e comprovar.
Um exemplo de pergunta para explorar com calma no seu computador:*

Neste caso use um prompt Estruturado com tags XML.

Problema: Considerando a ameaça quântica - Qual seria a Classificação de risco de um cenário fictício: uma fabricante de sensores industriais que retém dados de manutenção preditiva por 15 anos?

SEGUE UMA PROPOSTA DE PROMPT

Problema: Considerando a ameaça quântica - Qual seria a Classificação de risco de um cenário fictício: uma fabricante de sensores industriais que retém dados de manutenção preditiva por 15 anos?

<contexto> Você é um especialista em segurança pós-quântica aplicada a IoT industrial (Internet das Coisas Industrial). Está avaliando o caso de uma fabricante de sensores que retém dados de manutenção preditiva por 15 anos, coletados por dispositivos de baixa capacidade computacional (constrained devices: pouca energia, memória e processamento). **</contexto>**

<restricoes> - Os dispositivos não suportam algoritmos PQC (Post-Quantum Cryptography, criptografia pós-quântica) de footprint grande, como variantes lattice-based mais pesadas usadas em servidores.- O prazo de retenção de 15 anos, somado ao tempo de migração, supera o horizonte estimado até um computador quântico criptograficamente relevante (teorema de Mosca).- Migração criptográfica não pode ser tratada como projeto de médio prazo; trate como decisão operacional imediata. **</restricoes>**

<pergunta> Diante dessas restrições, quais algoritmos de PQC leve (lightweight PQC, adequados a dispositivos com recursos limitados) são hoje candidatos viáveis para proteger a telemetria desses sensores? Que arquitetura de crypto agility (capacidade de trocar algoritmos sem redesenhar o sistema) permitiria substituir esses algoritmos no futuro sem trocar o hardware instalado em campo? **</pergunta>**

<formato> Responda em três blocos:1. Diagnóstico de urgência, com base no teorema de Mosca aplicado a este caso específico.2. Até três algoritmos de PQC leve, com trade-offs de footprint (memória, energia, latência).3. Um primeiro passo concreto de crypto agility, executável em até 90 dias, sem substituição de hardware. **</formato>**

A Ameaça é Real, a Resposta já Existe

- **HNDL** torna o risco quântico uma vulnerabilidade ativa hoje, não uma hipótese de 2035.
- PQC é o caminho primário de proteção, já disponível em hardware clássico para IoT - QIoT tem QKD como complementar, para nichos em Internet Quântica.
- No próximo workshop: o que o mundo já exige em resposta, e o plano de ação que sua organização pode adotar rapidamente.



Ficou com alguma dúvida ou quer aprofundar um ponto? Continue conosco!!!



OBRIGADO!

Tempo Extra para dúvidas e network

Vamos continuar neste mesmo link – para quem desejar sair desejamos bom descanso.

Esta extensão se mostrou mais eficiente do que a com novo link.

