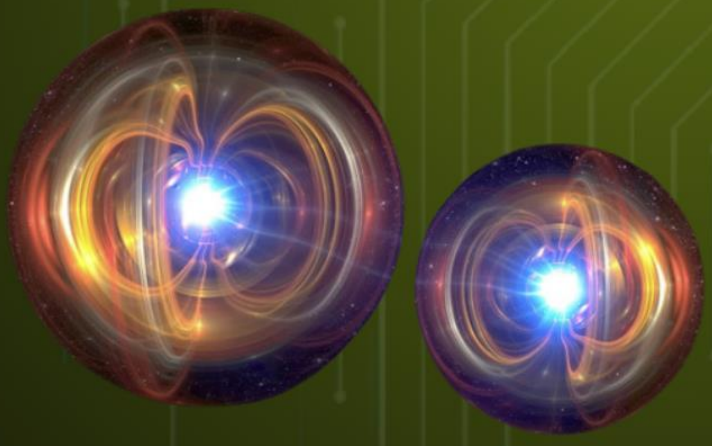
OS DESAFIOS DA INTERNET QUÂNTICA



ănima lab
hub

ÂNIMA EDUCAÇÃO

ÂNIMA HUB LAB – QUANTUMLAB

FÁBIO ARRUDA FREITAS – UNA DIVINOPOLIS

JÚLIA LUANA DE JESUS SOUZA – UNA BOM DESPACHO

JULIANA GERTRUDES DE OLIVEIRA – USJT

KAIQUE DE PAULA FERREIRA – UNA BOM DESPACHO

LEONARDO FELIPE MORAES SANTOS – UAM

LUIZ FERNANDO FERREIRA SANTO – UNA BOM DESPACHO

MARIA EDUARDA BARCELOS – UNA BOM DESPACHO

MIKAEL LIMA MAIA – USJT

NALANDA DUQUE DE SOUSA LIMA – USJT

RODRIGO CÍCERO FERREIRA DA CUNHA – UNA BOM DESPACHO

EBOOK: DESAFIOS DA INTERNET QUÂNTICA

SÃO PAULO 2024

Trabalho estudantil realizado com foco apresentar e desmistificar a Internet Quântica para toda a sociedade de uma forma interativa.

Em agradecimento especial a Professora Inês Brosso por toda orientação durante o desenvolvimento deste ebook.

SUMÁRIO

INTRODUÇÃO

Em um mundo cada vez mais interligado, a busca por uma comunicação mais segura, rápida e eficiente se torna urgente. E é exatamente isto que a Internet Quântica promete ofertar: revolucionar a maneira que nós nos comunicamos e interagimos com o mundo digital. Neste ebook, convidamos você a descobrir o que é um dos mais fascinantes fenômenos da atualidade: a Internet Quântica. Explicamos o que são a Internet Quântica, como eles funcionam, por que são revolucionários, e quais obstáculos e perspectivas impedirão o desenvolvimento do equipamento para o mercado.

A internet quântica é um campo em desenvolvimento que tem como objetivo criar uma rede de comunicação que utiliza princípios da mecânica quântica, como o entrelaçamento e a superposição. Isso pode permitir transmissões de dados ultra seguras e mais eficientes do que as redes convencionais, já que a informação quântica não pode ser copiada ou interceptada sem ser detectada. Embora a internet quântica ainda esteja nos estágios iniciais de pesquisa e desenvolvimento, ela tem o

potencial de revolucionar a forma como trocamos dados globalmente.

O QUE É A INTERNET QUÂNTICA?

A internet quântica baseia-se nas leis da física quântica, onde os dados ou informações que serão transmitidos sofrem as propriedades da física e mecânica quântica, que por sua natureza oferecem maior rapidez se comparado com as redes de computadores em uso hoje.

O século XXI apresenta uma série infinita de possibilidades e de desafios a serem desmistificados e compreendidos nos seus mais profundos segredos. Hoje mais do que nunca, com o multiplicar da ciência de forma exponencial, esta possibilidade se faz presente e mais próxima da nossa realidade diariamente. (BROSSO, FALBRIARD; 2020)

A física moderna desenvolveu-se em paralelo com a eletrônica e a construção de computadores, as descobertas sobre os átomos e partículas de menores grandezas, as quais comportam-se de maneira muito distinta de objetos do dia a dia levaram a conclusões de que esses sistemas físicos na verdade são governados por leis distintas da física clássica. A mecânica quântica proporcionou pesquisas na área da computação onde a escala para operação desses computadores seria de um átomo por bit, em que as suas operações elementares precisam ser descritas pela mecânica quântica. (SILVA; 2018).

Mecânica quântica são os fundamentos da física quântica que descreve o comportamento da natureza em escalas muito pequenas de nível atômico. Ajuda a explicar o comportamento da matéria juntamente com as suas interações com a energia. De acordo com Feynman que disse “A mecânica quântica lida com a natureza como ela é - absurda”. É amplamente aceito que as propriedades que a compõem são paradoxais e podem ser melhor explicadas através da matemática aplicada para que, então, possa-se ter um entendimento mais amplo a seu respeito. (REIS, 2020)

Entendidos tais conceitos a respeito da mecânica quântica, abordamos os computadores atuais cuja arquitetura é formada pela computação clássica, a qual leva em sua composição estruturas de circuitos extremamente pequenos em cada vez maior quantidade e 4 menores espaço físico, a Lei de Moore pode nos ajudar pois

explica que a estrutura atual está findada a um limite em um determinado período de tempo.

Lei de Moore criada pelo co-fundador da Intel Corporation Gordon Earl Moore, que no ano de 1965 escreveu um artigo científico prevendo que o número de transistores em um processador dobraria, em média, a

cada dois anos e mantendo o mesmo ou menor custo e um menor espaço. Assim sendo, a Lei de Moore baseia-se em uma observação a qual tornou-se uma projeção. Estes transistores são responsáveis pela maior parte dos processamentos de um computador ao estilo clássico da computação, processam informações e fazem operações lógicas.

Os computadores ficaram cada vez mais rápidos pelo aumento dos micro transistores nos microprocessadores, contudo este aumento progressivo não pode ser mantido no ritmo em que está. Pode-se concluir que a lei de Moore tem um limite, que é o próprio limite fundamental, ou seja, o tamanho de um transistor se igualar ao tamanho de um átomo. Com o fim inevitável da lei de Moore alternativas tiveram e foram pensadas, tal como a computação quântica, que dentre todas as alternativas é a mais provável a manter o progresso da ciência da computação. (LOOS;2021)

Vantagens:

1. **Segurança Aprimorada:** A criptografia quântica permite comunicações ultra seguras, já que qualquer tentativa de interceptação de dados alteraria o estado das partículas quânticas, sendo imediatamente detectada.

2. **Velocidade de Transmissão:** Com a possibilidade de transmissão de informações a velocidades próximas à da luz, a internet quântica pode aumentar significativamente a rapidez das comunicações.

3. **Capacidade de Processamento:** A internet quântica poderia conectar computadores quânticos, que têm um poder de processamento muito superior ao dos computadores tradicionais, permitindo a solução de problemas complexos de forma muito mais rápida.

4. **Entrelaçamento Global:** Poderíamos criar uma rede global de comunicação quântica, onde informações podem ser compartilhadas instantaneamente entre diferentes pontos do mundo.

Desvantagens:

1. **Complexidade Tecnológica:** A internet quântica envolve tecnologias altamente complexas, como qubits e entrelaçamento quântico. Construir e manter esses sistemas é desafiador e caro, o que torna o desenvolvimento lento.

2. **Fragilidade do Entrelaçamento:** O entrelaçamento quântico, que é essencial para a internet quântica, é muito frágil e facilmente interrompido por interferências externas, o que limita a distância de transmissão de dados.

3. **Infraestrutura Cara:** A criação de uma rede de internet quântica requer equipamentos altamente especializados, como repetidores quânticos e detectores sensíveis, o que aumenta os custos de implantação e manutenção.

4. **Distâncias Limitadas:** Atualmente, a transmissão de informações quânticas em longas distâncias é um grande desafio, pois o sinal quântico se deteriora rapidamente, e os repetidores quânticos ainda estão em desenvolvimento.

5. **Desafios na Correção de Erros:** A correção de erros quânticos é muito mais complicada do que em sistemas tradicionais, o que dificulta o processamento confiável de dados.

6. **Interoperabilidade Limitada:** Não há ainda padrões bem estabelecidos para garantir que diferentes sistemas quânticos possam se comunicar e operar de forma eficiente entre si, o que é necessário para expandir essa tecnologia.

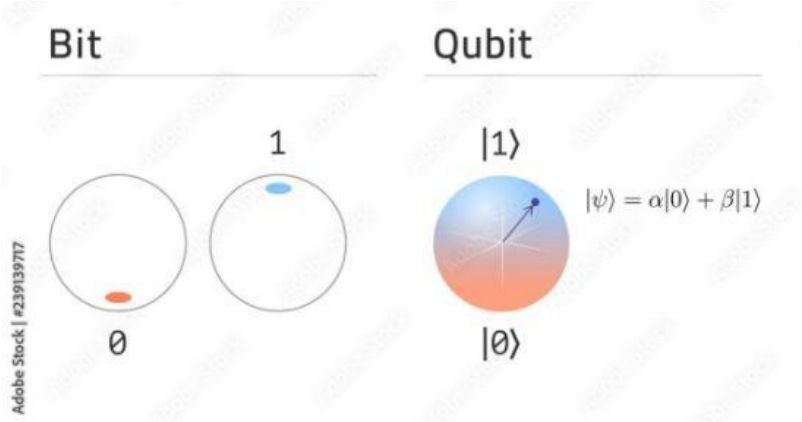
COMO FUNCIONA A INTERNET QUÂNTICA?

Uma dentre muitas das características intrínsecas à mecânica quântica e por consequência à computação quântica é o entrelaçamento quântico também conhecido como emaranhamento quântico que por sua vez, de forma resumida, funciona como um tipo de comunicação entre os pares quânticos ou os fótons como

é dito no artigo “O que é emaranhamento quântico? Tudo sobre essa peculiaridade ‘assustadora’ da física” onde é levado em consideração esta característica em que o par de partículas interagindo entre si podem descrever suas principais propriedades independente uma da outra. (ESTEFANSKI; 2022)

Com o desenvolvimento das pesquisas de superposição de estados e sobreposição quântica novos conhecimentos foram adquiridos levando a estudos para verificar os dois estados diferentes ao mesmo tempo. Levando a uma nova forma de transferir dados 6 através do que ficou conhecido como qubit. (BROSSO, FALBRIARD; 2020).

Outro dos elementos importantíssimos da computação quântica que é responsável pela troca de dados é o qubit (Quantum + bit) é o elemento central da computação quântica já que pode assumir o estado 0 e 1 ou ambos ao mesmo tempo, usando da sobreposição quântica em que os estados fundamentais são sobrepostos, como é dito no artigo científico “Introdução a computação quântica de Hamilton J. Brumatto - Unicamp”, a sobreposição é indicada por uma distribuição probabilística através dos estados fundamentais. Com esta propriedade do qubit, podendo trabalhar simultaneamente, aumenta–se consideravelmente a capacidade de processamento do computador, tornando-o seu processamento simultâneo. (BRUMATTO 2010).



Estado clássico do bit (lado esquerdo) comparado com o superposição quantum (a direita) bit **(Foto: por Astibuag Reprodução Adobe Stock - 2019)**

PROTOCOLOS QUÂNTICOS

A computação quântica, com seu potencial de realizar cálculos exponencialmente mais rápidos do que os computadores clássicos, representa uma ameaça significativa aos sistemas de segurança baseados em algoritmos criptográficos tradicionais, como RSA e ECC. Em resposta, a comunidade científica e organizações como o Instituto

Nacional de Padrões e Tecnologia (NIST) têm trabalhado no desenvolvimento de protocolos quânticos, que utilizam as propriedades da mecânica quântica para assegurar a integridade e a confidencialidade das comunicações (NIST, 2024).

Os protocolos quânticos utilizam fenômenos da mecânica quântica, como o emaranhamento e a superposição, para criar sistemas de segurança que são teoricamente invioláveis. Um exemplo notável é a **Distribuição de Chave Quântica (QKD)**, que permite a troca de chaves criptográficas entre duas partes de forma segura. Na QKD, qualquer tentativa de interceptação altera o estado quântico das partículas, alertando imediatamente as partes sobre a violação (NIST, 2023). Este princípio é amplamente estudado em sistemas baseados no protocolo BB84, desenvolvido por Charles Bennett e Gilles Brassard em 1984 (Bennett & Brassard, 1984).

A implementação de protocolos quânticos é uma prioridade em áreas sensíveis, como sistemas governamentais, financeiros e militares. Além disso, áreas emergentes, como a Internet das Coisas (IoT) e redes 5G, também se beneficiam desses avanços, garantindo comunicações seguras em ambientes com alta demanda de conectividade. Por exemplo, redes quânticas de teste estão sendo construídas em cidades como Tóquio, Xangai e Chicago, enquanto iniciativas como o Quantum Flagship na Europa e os programas do NIST nos Estados Unidos impulsionam o desenvolvimento e a padronização global (Quantum Flagship, 2024; NIST, 2023).

Embora a segurança baseada em protocolos quânticos seja atraente, desafios tecnológicos e econômicos dificultam sua ampla adoção. A infraestrutura necessária, como geradores de estados quânticos e detectores de fótons, ainda está em desenvolvimento e apresenta custos elevados. Além disso, implementar QKD em redes de longa distância depende de soluções como repetidores quânticos, que permanecem em estágio experimental (IBM, 2024). A coexistência com a infraestrutura clássica de segurança digital também exige investimentos significativos para adaptação (NIST, 2024).

Outro desafio é a coexistência dos protocolos quânticos com a infraestrutura clássica de segurança digital. Enquanto a criptografia pós-quântica (PQC) utiliza problemas matemáticos difíceis para computadores quânticos resolverem, os protocolos

quânticos exigem novos tipos de hardware, aumentando os custos e a complexidade (NIST, 2024).

O NIST e outras instituições lideram esforços para padronizar protocolos quânticos e integrar soluções pós-quânticas, garantindo que a infraestrutura global de segurança seja resiliente frente aos avanços da computação quântica. Além disso, há a necessidade de regulamentações globais para garantir o uso ético e seguro dessas tecnologias, especialmente em aplicações sensíveis, como redes governamentais e financeiras (Quantum Flagship, 2024; NIST, 2023).

O NIST também publicou diretrizes para a transição gradual de sistemas criptográficos tradicionais para soluções quânticas, incluindo a integração de protocolos quânticos com padrões de criptografia pós-quântica (NIST, 2024). Esses esforços buscam garantir que a infraestrutura global de segurança seja resiliente diante da evolução tecnológica.

Principais Categorias de Protocolos Quânticos

1. Distribuição de Chave Quântica (Quantum Key Distribution - QKD)

- **BB84**: O protocolo BB84, desenvolvido por Charles Bennett e Gilles Brassard em 1984, é o exemplo mais conhecido, e também o mais amplamente utilizado, de QKD (Quantum Key Distribution). Ele utiliza propriedades da mecânica quântica, como o princípio da incerteza e o colapso do estado quântico, para garantir a troca segura de chaves criptográficas entre duas partes. O BB84 é implementado em sistemas de alta segurança, como comunicações governamentais e financeiras (Bennett & Brassard, 1984). Sua aplicação em longas distâncias requer repetidores quânticos, que ainda estão em desenvolvimento (NIST, 2023).
- **B92**: O protocolo B92, uma simplificação do BB84, foi introduzido por Charles Bennett em 1992. Ele utiliza apenas dois estados quânticos, ao invés de quatro, para transmitir informações. Reduz a complexidade de implementação em relação ao BB84 e é mais suscetível a erros e ruídos no canal quântico (Bennett, 1992).
- **E91**: Proposto por Artur Ekert em 1991, o protocolo E91 utiliza o emaranhamento quântico para distribuir chaves seguras. Amplamente

estudado em redes quânticas e sistemas que requerem alta robustez contra ataques. A geração e o controle de pares emaranhados são tecnologicamente complexos e sensíveis a ruídos (Ekert, 1991).

- **Protocolo Lo-Chau**: Extensão do BB84 para incluir correção de erros e distilação de privacidade.

2. Protocolo de Teletransporte Quântico

- **Protocolo de Teletransporte de Bennett**: Transferência de um estado quântico de um ponto para outro usando pares emaranhados e comunicação clássica. Embora mais conhecidos na física fundamental, os protocolos de teletransporte quântico têm aplicações em segurança da informação. A sua aplicação se deve a criação de redes quânticas seguras para transferência de dados em sistemas governamentais e científicos (NIST, 2024).

3. Protocolo de Coin Tossing Quântico

- **Protocolo de Coin Tossing Quântico:** Este protocolo é utilizado para criar resultados aleatórios confiáveis em sistemas quânticos. Ele é particularmente útil para resolver disputas ou tomar decisões em sistemas distribuídos, incluindo tomada de decisões seguras em sistemas financeiros e jurídicos (IBM, 2024).
- **Protocolo de Blum**: Adaptado para o domínio quântico, usado para resolver disputas ou gerar aleatoriedade imparcial.
- **Protocolo Aharonov**: Propõe métodos para gerar resultados de maneira justa usando medições quânticas.

4. Protocolo de Segurança de Mensagem

- **Protocolo de Assinatura Digital Quântica (QDS)**: Usa estados quânticos para criar assinaturas seguras que são resistentes a alterações.
- **Protocolo BBM92**: Variante do BB84 aplicada à autenticação de mensagens.

5. Comunicação Quântica Direta

- **Protocolo Ping-Pong**: Permite comunicação bidirecional direta usando emaranhamento quântico.

- **Protocolo Wang et al.**: Usa QKD para comunicação direta sem chaves intermediárias.

6. Protocolo de Computação Segura e Verificação Quântica

- **Protocolo de Computação Multipartidária Segura**: Permite que várias partes realizem cálculos conjuntos sem expor seus dados.

Protocolo de Verificação Quântica de Computação (QCV): Garante que a computação realizada por um computador quântico seja correta e segura.

ONDE SE APLICAM AS TECNOLÓGIAS QUÂNTICAS?

As tecnologias quânticas começaram a transformar o mundo ainda no século XX, com aplicação do laser à medicina, na ressonância magnética, em aparelhos de cd, câmeras digitais, leitores de código de barras e em transistores e circuitos especiais de computadores. Neste século, os avanços se ampliaram no campo da fotônica quântica (exames de imagem), química quântica (diagnósticos rápidos e de baixo custo), desenvolvimento de novos materiais e abriram campo para a chamada de informação quântica. Em relação a estudos climáticos, surgiu uma nova geração de sensores quânticos para monitoramento ambiental e, em energias limpas, a possibilidade de células solares mais eficientes. A internet quântica, embora ainda em desenvolvimento, tem aplicações potenciais em várias áreas. Aqui estão algumas delas:

1. Segurança de Dados e Criptografia: A principal aplicação da internet quântica é a transmissão de dados ultra-segura. Com a criptografia quântica, como a distribuição de chaves quânticas (QKD), as informações são praticamente invioláveis, pois qualquer tentativa de interceptação altera o estado quântico, denunciando a tentativa.
Isso pode ser aplicado em setores que exigem alta segurança, como: ○ Governos (para comunicações diplomáticas e militares) ○ Setor financeiro (proteção de transações bancárias) ○ Indústria da saúde (segurança de prontuários médicos e informações sensíveis)

2. **Computação Quântica em Nuvem:** A internet quântica pode conectar computadores quânticos distantes, permitindo que eles compartilhem recursos e dados. Isso possibilitaria: ○ Computação colaborativa: Computadores quânticos em diferentes locais trabalhando juntos em problemas complexos, como simulações moleculares, criptografia avançada e inteligência artificial. ○ Soluções complexas: Pesquisa em novos medicamentos, otimização de logística e análise de grandes volumes de dados seriam aprimoradas com computadores quânticos interligados.

3. **Ciência e Pesquisa:** A internet quântica pode revolucionar o compartilhamento de dados científicos de forma rápida e segura. Áreas como: ○ Física e astrofísica (simulações e trocas de dados massivos) ○ Pesquisa genética (colaboração segura e instantânea entre laboratórios de pesquisa) ○ Meteorologia e mudanças climáticas (compartilhamento global de dados e simulações em tempo real)

4. **Defesa e Inteligência:** ○ Comunicações militares seguras: A internet quântica pode ser utilizada para proteger redes de comunicação militares e sistemas de comando e controle, onde a inviolabilidade é crítica. ○ Proteção contra espionagem: A criptografia quântica pode tornar as comunicações governamentais e de inteligência praticamente invulneráveis à espionagem.

5. **Telecomunicações e Redes de Comunicação:** Empresas de telecomunicações estão explorando a internet quântica para criar redes de comunicação seguras e eficientes. Isso pode ser aplicado em: ○ Redes de comunicação de longo alcance: A internet quântica pode criar canais de comunicação entre continentes, permitindo a troca de dados de forma segura entre diferentes partes do mundo. ○ Comunicação inter-satélites: A internet quântica poderia melhorar a segurança das comunicações entre satélites em órbita.

6. **Internet das Coisas (IoT):** No futuro, a internet quântica pode ser usada para proteger redes de IoT, garantindo que dispositivos conectados, como carros autônomos, casas inteligentes e sensores industriais, transmitam dados de maneira inviolável. Essas aplicações mostram o grande potencial da internet quântica em revolucionar a maneira como tratamos a segurança e a eficiência da comunicação e

do processamento de informações.

FORNECEDORES DE SUPRIMENTOS QUÂNTICOS

Um número cada vez maior de empresas de computação quântica está emergindo ao redor do mundo, dedicando-se ao desenvolvimento de processadores funcionais, bem como do hardware e software necessários para sua operação (INSIDER, 2023). Com o avanço da computação quântica e o desenvolvimento de protocolos quânticos, a necessidade de uma infraestrutura robusta e fornecedores especializados tornouse essencial. Esses fornecedores oferecem os elementos necessários para implementar tecnologias quânticas, como hardware, software, e serviços que suportam redes e sistemas baseados em princípios da mecânica quântica. Eles desempenham um papel crucial ao disponibilizar ferramentas que possibilitam a aplicação prática de protocolos quânticos, como a Distribuição de Chave Quântica (QKD) e a comunicação quântica direta (NIST, 2024). Fornecedores quânticos são empresas ou instituições que desenvolvem e comercializam produtos, serviços e tecnologias relacionados à computação e comunicação quântica. Seu portfólio abrange desde dispositivos físicos, como geradores de estados quânticos e detectores de fótons, até soluções integradas, como plataformas de criptografia quântica e infraestrutura para redes quânticas. Os fornecedores de suprimentos quânticos são fundamentais para impulsionar o avanço das tecnologias quânticas, fornecendo os componentes, dispositivos e materiais indispensáveis para pesquisas, desenvolvimento e aplicações práticas em diversas áreas. Esses suprimentos englobam uma ampla gama de produtos, desde sistemas de criogenia e lasers de alta precisão até detectores de fótons, chips quânticos e ferramentas de medição ultrassensíveis. Os fornecedores quânticos podem ser classificados de acordo com suas especializações, incluindo hardware quântico, software quântico e serviços baseados em nuvem. No segmento de hardware, são fornecidos dispositivos como processadores quânticos, geradores de estados emaranhados e detectores de partículas quânticas. No software, incluem-se ferramentas como simuladores quânticos e linguagens de programação, como Qiskit da IBM e Cirq do Google Quantum AI. Já os serviços em nuvem oferecem acesso remoto a plataformas quânticas, democratizando o uso de tecnologias quânticas para empresas de todos os portes (IBM, 2024). Existem também os fornecedores quânticos que também desenvolvem sistemas híbridos, capazes de operar com redes tradicionais e tecnologias quânticas emergentes (NIST, 2024). Além disso, esses fornecedores desempenham um papel essencial na transição para soluções pós-quânticas, desenvolvendo ferramentas que integram tecnologias

clássicas e quânticas. Empresas como a IBM, por exemplo, oferecem plataformas que suportam simultaneamente criptografia tradicional e protocolos quânticos, facilitando a adaptação de sistemas existentes. Isso é crucial para setores como finanças e defesa, onde a segurança de longo prazo é uma prioridade (NIST, 2023). Entre os principais fornecedores de tecnologias quânticas, destacam-se gigantes como IBM Quantum, Google Quantum AI, Alibaba Cloud e Toshiba. A IBM fornece plataformas de hardware e software baseadas em nuvem, enquanto a Google Quantum AI é reconhecida por seus avanços em hardware quântico, como o processador Sycamore, que alcançou a supremacia quântica em 2019. A Toshiba tem foco em soluções comerciais de QKD, e a Alibaba investe em redes quânticas e simuladores quânticos para aplicações industriais e governamentais (Google Quantum AI, 2024; IBM, 2024). Além dos grandes players, empresas emergentes como Rigetti Computing, D-Wave Systems e Pasqal têm contribuído significativamente para o mercado de tecnologias quânticas. A Rigetti foca no desenvolvimento de processadores baseados em supercondutores, enquanto a D-Wave é pioneira em computadores de recozimento quântico, voltados para problemas de otimização. Por outro lado, a Pasqal utiliza átomos neutros para desenvolver sistemas quânticos mais eficientes e compactos (Quantum Flagship, 2024). O aumento dos investimentos reflete a confiança no potencial transformador da computação quântica em diversos setores, como finanças, farmacêutico, logística e automotivo. Entre 2019 e 2022, o governo dos EUA investiu US$ 2,9 bilhões em tecnologias quânticas e planeja continuar ampliando esse aporte. Globalmente, países como Reino Unido, China e membros da UE também estão destinando bilhões de dólares para impulsionar o desenvolvimento quântico. No setor privado, os investimentos ultrapassaram US$ 2,35 bilhões em 2022, destacando o crescente interesse nas aplicações futuras dessa tecnologia emergente (FORBES, 2023). Com hardware e software especializados, os computadores quânticos prometem realizar tarefas que hoje estão além das capacidades dos computadores convencionais. Além disso, empresas do setor estão trabalhando ativamente no desenvolvimento de tecnologias que tornam essa inovação avançada mais acessível e fácil de usar (INSIDER, 2023). Atualmente, os benefícios frequentemente associados à computação quântica, como a quebra da criptografia, o desenvolvimento rápido de medicamentos revolucionários e soluções para problemas complexos de IA, ainda estão longe de se tornar realidade. Nesse cenário, as empresas do setor privado enfrentam o desafio de equilibrar as aplicações

práticas e imediatas da tecnologia com as promessas de seu potencial futuro, enquanto buscam justificar os investimentos realizados no campo (FORBES 2023). Apesar dos avanços, os fornecedores enfrentam desafios como o alto custo de produção e a necessidade de compatibilidade com infra estruturas clássicas. Por exemplo, a construção de detectores de fótons supercondutores requer materiais e processos altamente especializados, o que eleva os custos. Além disso, a integração de sistemas híbridos exige esforços significativos em pesquisa e desenvolvimento para garantir a interoperabilidade e a escalabilidade das soluções quânticas (NIST, 2024). O futuro dos fornecedores quânticos é promissor, com expectativas de crescimento acelerado do mercado global de computação quântica, que poderá ultrapassar US$ 65 bilhões até 2030. A redução de custos e a miniaturização de componentes serão fatores essenciais para a popularização das tecnologias quânticas, enquanto parcerias público-privadas, como o programa europeu Quantum Flagship, continuarão a impulsionar a inovação e a adoção dessas tecnologias em larga escala (Quantum Flagship, 2024).

PRINCIPAIS COMPONENTES DE SUPRIMENTOS QUÂNTICOS

Os fornecedores atendem a demandas variadas que incluem desde dispositivos básicos até sistemas avançados de comunicação quântica. Alguns dos principais componentes fornecidos incluem: 1. Geradores de Estados Quânticos: Utilizados para criar fótons polarizados e estados quânticos emaranhados. Esses dispositivos são cruciais para protocolos como BB84 e E91 (Bennett & Brassard, 1984; Ekert, 1991). 2. Detectores de Fótons: Equipamentos altamente sensíveis que detectam partículas quânticas para decodificar informações em protocolos de QKD. Sua eficiência afeta diretamente a taxa de sucesso das transmissões (NIST, 2023). 3. Repetidores Quânticos: Permitindo a amplificação e retransmissão de sinais quânticos, eles são fundamentais para a implementação de redes quânticas de longa distância, ainda em desenvolvimento (Quantum Flagship, 2024). PRINCIPAIS FORNECEDORES QUÂNTICOS Enquanto o cenário da computação quântica está repleto de startups inovadoras, os principais fornecedores de computação quântica estão na vanguarda da tecnologia, impulsionando inovações em hardware, software e soluções aplicadas à computação, criptografia, simulação de materiais, inteligência artificial e muitos outros campos. Esses fornecedores, que incluem gigantes tecnológicos e startups

especializadas, estão desenvolvendo e oferecendo tecnologias quânticas que podem transformar diversos setores, desde a saúde até a segurança cibernética. (FORBES 2023) Os avanços na fabricação de dispositivos quânticos e na redução de custos prometem ampliar o acesso às tecnologias quânticas. Parcerias entre grandes empresas e governos, como o programa europeu Quantum Flagship e os investimentos chineses em infraestrutura quântica, continuam a impulsionar o setor (Quantum Flagship, 2024). Além disso, iniciativas de padronização lideradas pelo NIST garantem que os fornecedores atendam a requisitos internacionais de segurança e interoperabilidade (NIST, 2024). 1. IBM Quantum: A IBM oferece plataformas quânticas baseadas em nuvem que permitem acesso a hardware quântico, além de suporte para integração com redes tradicionais (IBM, 2024). A empresa também fornece soluções para implementação de protocolos quânticos em setores governamentais e financeiros. 2. ID Quantique: Sediada na Suíça, a ID Quantique é uma das líderes globais em tecnologias de criptografia quântica e QKD. A empresa fornece dispositivos como módulos de QKD e geradores de números aleatórios baseados em fenômenos quânticos, utilizados em sistemas de alta segurança (ID Quantique, 2023). 3. Google Quantum AI: A Google Quantum AI lidera esforços no desenvolvimento de hardware quântico avançado e plataformas de simulação. Seu processador "Sycamore" alcançou a "supremacia quântica" em 2019, demonstrando o potencial da computação quântica para resolver problemas complexos (Google, 2024). A empresa também oferece suporte para desenvolvimento de algoritmos quânticos e pesquisa em protocolos de segurança quântica, promovendo a integração dessas tecnologias em aplicações práticas. 4. Alibaba Cloud Quantum Computing: A divisão quântica da Alibaba fornece serviços em nuvem que incluem simuladores quânticos e hardware para testes de protocolos de comunicação quântica. Também investe no desenvolvimento de redes quânticas em parceria com instituições chinesas (Quantum Flagship, 2024). 5. Toshiba Quantum Key Distribution (QKD): A Toshiba desenvolveu sistemas de QKD comerciais, permitindo a implementação de segurança quântica em redes de telecomunicações (Toshiba, 2023). A empresa está focada na criação de infraestrutura para redes 5G e IoT seguras. 6. Intel : Recentemente, a empresa lançou o chip Tunnel Falls, um processador quântico de silício com 12 qubits, com foco no avanço da pesquisa de qubits de spin de silício. A Intel planeja integrar esse chip à sua pilha quântica completa, que incluirá o Intel Quantum Software Development Kit (SDK), facilitando o

desenvolvimento de software quântico. Desafios para os Fornecedores Apesar do avanço, os fornecedores de suprimentos quânticos enfrentam desafios significativos, como: ● Custo de Produção: Componentes quânticos são caros devido à necessidade de precisão extrema e materiais avançados, como detectores supercondutores (NIST, 2024). ● Compatibilidade com Infraestrutura Clássica: Integração entre dispositivos quânticos e sistemas clássicos é uma barreira, especialmente em redes híbridas (IBM, 2024). ● Escalabilidade: A ampliação para redes globais requer repetidores quânticos mais eficientes e sistemas de menor custo (Quantum Flagship, 2024).

A INTERNET QUÂNTICA HOJE

A Internet Quântica ainda está em estágio de desenvolvimento, mas se encontra em um estágio empolgante. Com o passar dos anos, foram feitos avanços significativos em seu desenvolvimento, mas ainda há muitos desafios a serem superados antes que essa tecnologia se torne realidade e esteja ao alcance do público geral.

Aqui estão alguns dos principais marcos recentes:

Em 2022: Cientistas chineses realizaram com sucesso a primeira transmissão quântica intercontinental, conectando a China à Áustria.

Em 2023: Pesquisadores da IBM demonstraram um repetidor quântico funcional, um componente crucial para a construção de redes quânticas de longo alcanc**e.**

Em 2024: Uma equipe do Google conseguiu teletransportar informações quânticas com sucesso a uma distância de 100 quilômetros.

(GEMINI, GOOGLE - Acesso feito em 12/05/2024)

PORTAS LÓGICAS QUÂNTICAS

As muitas operações necessárias na computação, são feitas a partir de portas lógicas. Existe um conjunto reduzido de portas que, combinadas, são capazes de produzir qualquer operação lógica. As portas que pertencem a esse conjunto são chamadas

portas universais. As portas universais clássicas, ou seja, da computação clássica, são compostas pela combinação de três portas: AND, OR, NOT. Fazendo uma combinação dessas portas foi possível criar outras duas novas portas, NAND e NOR, essas são muito úteis à universalidade. Para a computação quântica também temos um conjunto de portas lógicas quânticas que são capazes realizar computação quântica universal. (SOUZA,R.C.Portas lógicas quânticas universais para o grau de liberdade de caminho da luz.Rio de Janeiro.2021)

As portas quânticas diferente das portas lógicas clássicas precisam de mais valores de saída, não apenas um, porque com os estados em emaranhamento, precisamos medir todos os qubits. As portas quânticas são matrizes unitárias, ou seja, elas são reversíveis, uma matriz reversível quer dizer que uma matriz multiplicada pela sua transposta resulta na própria matriz, salvando assim o resultado dos qubits. (NASCIMENTO. Eduardo ,P. L.Arquitetura de Computadores Quânticos e Implementação de Portas Lógicas Quânticas em Ambiente 3D.São Paulo.2021)

É uma prática comum na ciência da computação quântica usar o mesmo termo “bit” para descrever o sistema clássico de dois estados que representa o valor do bit abstrato. Mas este uso de um único termo para caracterizar tanto o bit abstrato (0 ou 1) quanto o sistema físico cujo dois estados representam os dois valores é uma fonte potencial de confusão.Para evitar tal confusão, usarei o termo Cbit (“C” para “clássico”) para descrever o sistema físico clássico de dois estados e Qubit para descreva sua generalização quântica.

Representaremos o estado de cada Cbit como uma espécie da caixa, representada pelo símbolo | , no qual colocamos o valor 0 ou 1, representado por esse estado. Assim, os dois estados distinguíveis de um Cbit são representados pelos símbolos |0 e |1. É o comum pratique chamar o próprio símbolo |0 ou |1 de estado do Cbit, assim usando o mesmo termo para se referir tanto à condição física. (QUANTUM COMPUTER SCIENCE: AN INTRODUCTION.MERMIN,David..2007)

Existem portas quânticas que operam com apenas um qubit e portas quânticas que operam com mais qubits. Serão exemplificadas a seguir algumas portas lógicas comumente conhecidas:

1. **Porta Hadamard (H):**

   Possui a interessante propriedade de mapear um qubit |0) ou |1}) numa sobreposição de estados:

|0) = |0) + |1)2 e |1) = |0) - |1)2

2. **Porta Pauli (X, Y, Z):**

   Atua sobre um qubit e é equivalente a uma operação de NOT:

   |0) = |1) e |1) = |0)

3. **Porta CNOT (Controlled-NOT):**

   Atua sobre dois ou mais qubits. Para o caso de dois qubits, realiza uma operação similar à da porta Pauli-X no segundo qubit se o primeiro qubit for 1, e não os altera se o primeiro for 0:

   |00) = |00), |01) = |01), |10) = |11) e |11) = |10)

4. **Porta Toffoli (CCNOT):**

   É uma porta que atua sobre três qubits e possui uma propriedade muito relevante: é universal do ponto de vista de implementação de qualquer função booleana. Sua atuação pode ser expressa da seguinte maneira:

   |a,b,c) = a,b,cab)

(FUNDAMENTOS DA COMPUTAÇÃO QUÂNTICA.BAPTISTA,David Felice.São Paulo.2022)

De forma geral, o uso prático das portas iria para além do habitual, podendo viabilizar situações como a implementação de algoritmos eficientes, como a Transformada de Fourier Quântica, crucial para fatoração de números grandes, a suportação de protocolos quânticos de segurança, como o BB84, ao manipular estados entrelaçado, e entre outras inúmeras simulações envolvendo um enorme número de dados.

O QUE É CRIPTOGRAFIA QUÂNTICA?

A criptografia quântica se refere a vários métodos de cibersegurança para criptografar e transmitir dados seguros com base nas leis naturalmente ocorrentes e imutáveis da mecânica quântica (IBM, 2024).

Embora ainda esteja em seus estágios iniciais, a criptografia quântica tem o potencial de ser muito mais segura do que os tipos anteriores de algoritmos criptográficos e é até teoricamente impossível de hackeada (IBM, 2024).

Ao contrário da criptografia tradicional, que é construída sobre matemática, a criptografia quântica é construída sobre as leis da física. Especificamente, criptografia quântica depende dos princípios únicos da mecânica quântica (IBM, 2024):

- As partículas são inerentemente incertas: No nível quântico, as partículas podem existir ao mesmo tempo em vários lugares ou em vários estados de ser, e é impossível prever com precisão seu estado quântico (IBM, 2024).
- Os fótons podem ser medidos aleatoriamente em posições binárias: os fótons, as menores partículas de luz, podem ser configurados com polaridades ou giros específicos, que podem servir como um equivalente binário para os uns e zeros dos sistemas computacionais clássicos (IBM, 2024).
- Um sistema quântico não pode ser medido sem ser alterado: de acordo com as leis da física quântica, o ato básico de medir ou até mesmo observar um sistema quântico sempre terá um efeito mensurável nesse sistema (IBM, 2024).
- As partículas podem ser clonadas parcialmente, mas não totalmente: embora as propriedades de algumas partículas possam ser clonadas, acredita-se que um clone 100% seja impossível (IBM, 2024).

Por que criptografia quântica é importante?

Até o momento, a tradicional criptografia de dados geralmente tem sido suficiente para manter comunicações seguras na maioria das configurações de segurança cibernética (IBM, 2024).

No entanto, a ascensão da computação quântica representa uma ameaça existencial até para os algoritmos criptográficos tradicionais mais seguros. Como a criptografia quântica, a computação quântica é uma tecnologia de rápida evolução que também aproveita as leis da mecânica quântica (IBM, 2024).

Em comparação com nossos computadores clássicos mais rápidos e avançados, os computadores quânticos têm o potencial de resolver problemas complexos em ordens de grandeza mais rápidas (IBM, 2024).

O matemático Peter Shor descreveu pela primeira vez a ameaça que os computadores quânticos representam para os sistemas de segurança tradicionais em 1994. Os sistemas criptográficos de hoje podem ser divididos em duas categorias principais: sistemas simétricos, que usam uma chave secreta para tanto criptografar quanto descriptografar dados, e sistemas assimétricos, que usam uma chave pública que qualquer um pode ler e chaves privadas que apenas partes autorizadas podem acessar. Ambos os tipos de sistemas criptográficos criam essas chaves multiplicando grandes números primos e contam com o enorme poder de computação necessário para fatoração de grandes números para garantir que essas chaves de criptografia não possam ser quebradas por espiões ou hackers (IBM, 2024).

Mesmo os supercomputadores mais poderosos do mundo exigiriam milhares de anos para quebrar matematicamente algoritmos de criptografia modernos, como o Advanced Encryption Standard (AES) ou o RSA. Conforme o Algoritmo de Shor, fatorar um número grande em um computador clássico exigiria uma quantidade tão grande de poder computacional que um hacker levaria muitas vidas antes de se aproximar, mas um computador quântico completamente funcional, caso seja aperfeiçoado, poderia, teoricamente, encontrar a solução em apenas alguns minutos (IBM, 2024).

Os casos de uso para criptografia quântica são tão infinitos quanto existem casos de uso para qualquer forma de criptografia. Caso algo, desde informações corporativas até segredos estatais, deva ser mantido seguro, quando a computação quântica torna obsoletos algoritmos criptográficos existentes, a criptografia quântica pode ser nosso único recurso para proteger dados privados (IBM, 2024).

Como cientistas da computação em todo o mundo trabalham dia e noite para desenvolver tecnologia quântica prática, é fundamental que também desenvolvamos novas formas de criptografia para nos prepararmos para a era quântica da computação. Embora os computadores quânticos fossem considerados apenas teóricos no passado, especialistas estimam que podemos estar a apenas 20 a 50 anos de entrar plenamente na era quântica (IBM, 2024).

Tipos de criptografia quântica

- Distribuição quântica de chaves (QKD)

Originalmente teorizado em 1984 por Charles H. Bennett (do Thomas J. Watson Research Center da IBM) e Gilles Brassard, a distribuição quântica de chaves (QKD) é o tipo mais comum de criptografia quântica. Os sistemas QKD não são normalmente usados para criptografar os próprios dados seguros, mas sim para realizar uma troca segura de chaves entre duas partes, construindo colaborativamente uma chave privada compartilhada que, por sua vez, pode ser usada para métodos tradicionais de criptografia com chave simétrica (IBM, 2024).

Os sistemas QKD funcionam enviando partículas de luz de fóton individuais através de um cabo de fibra óptica. Este fluxo de fótons viaja em uma única direção e cada um representa um bit único, ou qubit, de dados—zero ou um. Os filtros polarizados no lado do remetente alteram a orientação física de cada fóton para uma posição específica, e o receptor usa dois divisores de feixe disponíveis para ler a posição de cada fóton conforme são recebidos. O remetente e o receptor comparam as posições de fótons enviados com as posições descodificadas, e o conjunto que corresponde se torna a chave (IBM, 2024).

- Quantum coin-flipping

Quantum coin-flipping é um tipo primitivo de criptografia (algo como um bloco de construção para algoritmos) que permite que duas partes que não confiam umas nas outras entrem em um acordo com base em um conjunto de parâmetros. Imagine se Bob e Alice estão falando ao telefone e querem apostar no cara e coroa, mas apenas Bob tem acesso à moeda. Se Alice aposta cara, como pode ter certeza de que Bob não vai mentir e dizer que o resultado foi coroa, mesmo que caia cara (IBM, 2024)?

- Outros tipos de criptografia quântica

Os pesquisadores continuam explorando outros tipos de criptografia quântica que incorporam criptografia direta, assinaturas digitais, entrelaçamento quântico e outras formas de comunicação quântica. Outros tipos de criptografia quântica incluem o seguinte (IBM, 2024):

- Criptografia quântica baseada em posição (IBM, 2024)
- Criptografia quântica independente da dispositivo (IBM, 2024)
- Protocolo kek (IBM, 2024)
- Protocolo Y-00 (IBM, 2024)
- **Criptografia pós-quântica**

De acordo com o National Institute of Standards and Technology (NIST) (link externo ao site ibm.com), o objetivo da criptografia pós-quântica (PQC, também chamada de resistente a tecnologia quântica ou seguro contra a tecnologia quântica) é "desenvolver sistemas de criptografia que são seguros contra computadores quânticos e clássicos, e podem interoperar com protocolos e redes de comunicação existentes" (IBM, 2024).

Não deve ser confundido com criptografia quântica, que depende das leis naturais da física para criar sistemas criptográficos seguros, algoritmos de criptografia pósquântica usam diferentes tipos de criptografia para criar segurança à prova quântica (IBM, 2024).

Estas são as seis áreas primárias da criptografia quântica segura (IBM, 2024):

- Criptografia baseada em rede (IBM, 2024)
- Criptografia multivariada (IBM, 2024)
- Criptografia baseada em hash (IBM, 2024)
- Criptografia baseada em código (IBM, 2024)
- Criptografia baseada em isogenia (IBM, 2024)
- Resistência quântica de chave simétrica (IBM, 2024)

Quando os dados confidenciais da sua organização são acessados, armazenados e transmitidos em ambientes híbridos e multinuvem, é necessário uma proteção excepcional para mantê-los seguros (IBM, 2024).

As soluções de criptografia combinam tecnologias, integração de sistemas e serviços de segurança gerenciados para garantir agilidade criptográfica, segurança quântica e políticas sólidas de governança e gerenciamento de riscos (IBM, 2024).

CRIPTOGRAFIA PÓS-QUÂNTICA

De acordo com o NIST (National Institute of Standards and Technology em inglês, Instituto Nacional de Padrões e Tecnologia dos EUA), algoritmos de criptografia protegem informações eletrônicas confidenciais de acessos de visualizadores não autorizados (NIST, 2024). Entretanto, apesar desses algoritmos terem sido o suficiente para defender ataques realizados por computadores convencionais por algumas décadas, os computadores quânticos, um novo tipo de dispositivo em desenvolvimento, podem quebrar esses algoritmos, sendo capazes de resolver os complexos problemas matemáticos nos quais esses algoritmos se baseiam e assim tornando os dados eletrônicos antes considerados seguros vulneráveis à descoberta (NIST, 2022).

Ainda segundo o NIST, para mitigar e combater essa ameaça iminente, se torna necessário o desenvolvimento de métodos criptográficos, ou seja, de algoritmos de criptografia que sejam resistentes tanto a ataques de computadores convencionais quanto aos futuros computadores quânticos. Esses novos algoritmos são chamados de algoritmos de criptografia pós-quântica (NIST, 2023)..

A criptografia pós-quântica (PQC, do inglês Post-Quantum Cryptography) é um campo emergente que visa a criação de algoritmos de segurança digital robustos o suficiente para garantir segurança digital enquanto resistem ao potencial poder de processamento dos computadores quânticos. Estes dispositivos, ao contrário dos convencionais, exploram propriedades da física quântica, como a superposição e o emaranhamento, permitindo a resolução de problemas matemáticos complexos de maneira exponencialmente mais rápida (NIST, 2022). Esta capacidade representa uma ameaça direta aos algoritmos de criptografia assimétrica atuais, como RSA e ECC (criptografia de curva elíptica), amplamente utilizados para proteger dados confidenciais e transações digitais (NIST, 2024).

Conforme o NIST, para evitar ataques de um computador quântico e proteger contra esses possíveis ataques — caso um modelo “criptograficamente relevante” seja construído no futuro — a comunidade global precisa substituir os algoritmos de criptografia atuais. Algoritmos de criptografia pós-quântica (PQC) devem se basear em problemas matemáticos complexos que seriam desafiadores tanto para computadores convencionais quanto para computadores quânticos resolverem (Federal Register, 2024).

Esses algoritmos foram desenvolvidos para atender a duas necessidades principais de segurança digital: criptografia geral, usada para proteger dados trocados em redes públicas, como senhas, e assinaturas digitais, essenciais para autenticação de identidade (NIST, 2023).

Segundo o NIST, dos quatro algoritmos iniciais selecionados para padronização, três são baseados em problemas matemáticos de reticulados estruturados, enquanto o quarto se baseia em funções hash, que utilizam estruturas matemáticas diferentes das usadas para fatoração de grandes números. Essas abordagens foram projetadas para serem difíceis de resolver tanto por computadores quânticos quanto por computadores convencionais (NIST, 2022).

Além dos quatro algoritmos principais, outros algoritmos adicionais estão sendo avaliados para futuras padronizações, oferecendo alternativas para a criptografia geral que não se baseiam em reticulados estruturados ou funções hash. Com o objetivo de colocar esses algoritmos em prática, o NIST lidera a criação de padrões técnicos para a criptografia pós-quântica, com foco em fornecer soluções que atendam diferentes contextos e permitam uma variedade de abordagens de segurança, garantindo mais de uma opção para cada tipo de aplicação, caso uma delas demonstre vulnerabilidades no futuro (NIST, 2023).

O NIST (Instituto Nacional de Padrões e Tecnologia dos EUA) lançou, em 2016, uma iniciativa para identificar, desenvolver e padronizar algoritmos que garantam a segurança contra ataques de computadores quânticos, visando assegurar a privacidade e integridade de dados a longo prazo. Esta medida é essencial, pois a implementação de novos sistemas de criptografia em larga escala pode levar décadas, e estima-se que computadores quânticos capazes de quebrar a criptografia convencional possam surgir nas próximas duas décadas (NIST, 2023).

O projeto de Criptografia Pós-Quântica do NIST começou em 2016, quando a instituição formalizou um convite global para que especialistas em criptografia

enviassem algoritmos capazes de resistir tanto a ataques de computadores convencionais quanto de computadores quânticos. Cerca de um ano depois, o prazo final trouxe a inscrição de 69 algoritmos candidatos de diversas partes do mundo, todos alinhados com os critérios de segurança estabelecidos pelo NIST (Federal Register, 2024).

Após o recebimento das submissões, o NIST divulgou publicamente esses algoritmos para que especialistas em criptografia os avaliassem e tentassem quebrá-los, em um processo completamente aberto e transparente. Ao longo dos anos seguintes, criptógrafos renomados participaram de múltiplas rodadas de análise rigorosa, o que gradualmente reduziu o número de candidatos e ajudou a refinar os algoritmos mais promissores (NIST, 2024).

O NIST também incentivou os criptógrafos a considerar a aplicação dos algoritmos em dispositivos com diferentes capacidades de processamento. Além de computadores e smartphones, dispositivos menores e com poder de processamento limitado, como cartões inteligentes, dispositivos domésticos conectados à Internet das Coisas (IoT) e microchips individuais, também precisam de algoritmos que sejam resistentes a ataques quânticos (também chamados de quantum) para garantir a segurança digital no futuro (NIST, 2023).

Após várias rodadas de testes e avaliações rigorosas, conduzidas ao longo de seis anos, o NIST anunciou, em 2022, os primeiros quatro algoritmos selecionados para padronização: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON e SPHINCS+ (NIST, 2022).

A criptografia pós-quântica marca uma nova era na segurança digital, oferecendo soluções que garantem a integridade e a confidencialidade dos dados em um futuro com computadores quânticos. Com a padronização dos primeiros algoritmos resistentes a ataques quânticos, o NIST está liderando o caminho para proteger informações críticas, antecipando-se a ameaças tecnológicas. A preparação para o cenário pós-quântico é essencial para proteger a infraestrutura digital global e preservar a privacidade em um mundo cada vez mais digitalizado (NIST, 2024). A transição para algoritmos de criptografia pós-quântica impactará uma vasta gama de setores. Na área financeira, por exemplo, a integridade das transações e dados confidenciais será reforçada contra possíveis ataques quânticos. No setor governamental e na saúde, onde informações sigilosas e dados pessoais são altamente valiosos, a PQC será crucial para garantir a segurança de longo prazo. A

implementação dos novos padrões PQC deve começar o mais cedo possível, pois a adaptação de sistemas legados pode ser demorada e complexa (NIST, 2023). O impacto da PQC será sentido em vários níveis: desde a segurança de transações bancárias e comunicação pessoal até o armazenamento de dados governamentais e militares. Especialistas recomendam que empresas e instituições comecem a adotar esses algoritmos em seus sistemas para garantir que estejam protegidas contra a ameaça iminente dos computadores quânticos (NIST, 2024).

Embora o NIST tenha selecionado um conjunto inicial de algoritmos, a transição completa para a criptografia pós-quântica representa um desafio significativo. A adaptação de sistemas existentes e a integração desses novos padrões demandam tempo e recursos. O NIST também continuará avaliando algoritmos alternativos, como BIKE e Classic McEliece, para garantir que existam soluções de backup robustas (NIST, 2023).

Para título de informação, de acordo com o NIST, embora os nomes pareçam semelhantes, criptografia pós-quântica e criptografia quântica são conceitos distintos com abordagens diferentes para a segurança digital. A criptografia pós-quântica (PQC) é uma defesa projetada para resistir a ataques de computadores quânticos, utilizando algoritmos matemáticos, muitos dos quais têm raízes históricas profundas, como as curvas elípticas, que datam de períodos antigos. Esses algoritmos são ajustados para serem seguros contra a capacidade de processamento quântico, mantendo-se aplicáveis em sistemas tradicionais (NIST, 2022).

A criptografia quântica, por outro lado, se baseia diretamente nas propriedades da mecânica quântica, que surgiu no século XX. Ela utiliza fenômenos quânticos, como o emaranhamento e a superposição, para criar métodos de segurança completamente novos e teoricamente invioláveis, como a distribuição de chave quântica (QKD). Embora ambos os tipos de criptografia busquem segurança contra o poder dos computadores quânticos, a criptografia quântica alcança isso de maneira fundamentalmente diferente ao usar as leis da física, enquanto a criptografia pós quântica depende de problemas matemáticos que são difíceis tanto para computadores clássicos quanto para computadores quânticos resolverem (NIST, 2024).

Seleção dos Primeiros Algoritmos de Criptografia Resistentes a Computadores Quânticos pelo NIST

Em julho de 2022, o NIST anunciou a seleção dos primeiros quatro algoritmos de criptografia pós-quântica como parte de sua iniciativa para proteger dados contra potenciais ataques de computadores quânticos. Os algoritmos selecionados são CRYSTALS-Kyber para criptografia geral e CRYSTALS-Dilithium, FALCON, e SPHINCS+ para assinaturas digitais. CRYSTALS-Kyber foi escolhido por sua eficiência na troca de chaves com tamanhos compactos, ideal para comunicações seguras. Para assinaturas digitais, CRYSTALS-Dilithium e FALCON são recomendados pela alta eficiência em verificação de identidade, enquanto SPHINCS+ usa uma abordagem baseada em hash, garantindo uma alternativa segura que não depende de reticulados estruturados (NIST, 2022).
Esses algoritmos foram escolhidos após uma avaliação rigorosa, que incluiu criptógrafos internacionais, visando oferecer uma defesa robusta contra a ameaça quântica. O NIST recomenda que organizações e especialistas em segurança comecem a preparar suas infraestruturas para a transição, revisando os sistemas que dependem de criptografia pública e incentivando equipes de TI a se familiarizarem com as novas tecnologias (NIST, 2022).

Os algoritmos selecionados pelo NIST foram divididos em duas categorias principais: Criptografia para Estabelecimento de Chaves e Assinaturas Digitais. Abaixo, uma descrição breve de cada algoritmo escolhido (NIST, 2022).

- CRYSTALS-Kyber: Este algoritmo, baseado em redes estruturadas, é projetado para troca de chaves em redes públicas. Sua estrutura matemática complexa e o uso de chaves de tamanho relativamente pequeno o tornam ideal para aplicações de segurança em tempo real, como redes públicas e dispositivos IoT (NIST, 2022).
- CRYSTALS-Dilithium: Também baseado em redes, CRYSTALS-Dilithium é uma solução de assinatura digital que combina segurança e eficiência, sendo ideal para aplicações que exigem autenticação robusta e integridade de dados.

O NIST recomenda este algoritmo como a principal opção de assinatura digital para ambientes pós-quânticos (NIST, 2022).

- FALCON: Outro algoritmo de assinatura digital baseado em redes, o FALCON é otimizado para dispositivos com restrições de hardware, como dispositivos IoT. Ele oferece uma alternativa ao Dilithium em cenários onde a eficiência em processamento e espaço é uma prioridade (NIST, 2022).
- SPHINCS+: Ao contrário dos algoritmos baseados em redes, SPHINCS+ utiliza funções hash para a geração de assinaturas digitais. Este algoritmo foi escolhido como uma opção complementar aos métodos baseados em redes, oferecendo segurança adicional em caso de vulnerabilidades nos algoritmos de rede no futuro (NIST, 2022).

Detalhamento dos Padrões FIPS 203, 204 e 205: Um Avanço na Criptografia PósQuântica

O lançamento dos padrões FIPS 203, 204 e 205 pelo NIST representa um marco essencial na segurança de dados para uma era de computação quântica. Esses padrões foram desenvolvidos ao longo de oito anos para oferecer proteção contra ameaças tanto de computadores convencionais quanto de futuros computadores quânticos. Cada padrão foi projetado com uma função específica, atendendo a duas necessidades principais: troca segura de chaves e assinaturas digitais confiáveis (Federal Register, 2024).

- FIPS 203 – Encapsulamento de Chaves Baseado em Reticulados Modulares (CRYSTALS-Kyber): O FIPS 203 especifica um esquema de encapsulamento de chave utilizando estruturas de reticulados modulares, derivado do algoritmo CRYSTALS-Kyber. Esse sistema é voltado para proteger a troca de chaves em redes públicas e é projetado para fornecer segurança robusta com uso eficiente de recursos. CRYSTALS-Kyber foi selecionado por ser altamente eficaz para redes de baixa latência, garantindo que a troca de chaves permaneça segura mesmo com o avanço da computação quântica. A estrutura modular torna-o ideal para dispositivos com diferentes capacidades de

processamento, incluindo IoT e sistemas críticos que requerem resiliência de longo prazo (NIST, 2024).

- FIPS 204 – Assinaturas Digitais Baseadas em Reticulados Modulares (CRYSTALS-Dilithium): O FIPS 204 define um padrão para assinaturas digitais utilizando reticulados modulares, com base no algoritmo CRYSTALS-Dilithium. Este padrão é destinado a fornecer uma solução confiável para autenticação de identidade e integridade de dados. O CRYSTALS-Dilithium se destaca pela eficiência em verificação de assinaturas, sendo recomen dado para aplicações que demandam autenticação frequente e em larga escala. Além de garantir segurança robusta, esse padrão permite que assinaturas sejam verificadas rapidamente, o que o torna aplicável em diversos setores, incluindo o financeiro e o governamental, onde a verificação constante de identidade é crítica (NIST, 2024).
- FIPS 205 – Assinaturas Digitais Baseadas em Funções Hash (SPHINCS+): O FIPS 205 oferece uma abordagem alternativa com base em funções hash, com o algoritmo SPHINCS+. Este padrão foi projetado para oferecer segurança adicional como uma alternativa independente dos reticulados, sendo uma opção complementar para casos em que a durabilidade de longo prazo é necessária. SPHINCS+ utiliza assinaturas sem estado e baseadas em hash, que são inerentemente resistentes a ataques quânticos. Essa abordagem é ideal para cenários que exigem segurança contra uma ampla gama de possíveis vulnerabilidades, proporcionando uma camada adicional de proteção em sistemas de alto valor e com dados extremamente sensíveis (NIST, 2024).

Esses três padrões representam o compromisso do NIST em desenvolver soluções seguras e interoperáveis, prontas para serem implementadas em diversas plataformas, desde grandes centros de dados até pequenos dispositivos de IoT e microchips. Eles são projetados para serem altamente adaptáveis, assegurando que sistemas de diferentes capacidades possam migrar gradualmente para essa tecnologia, garantindo a proteção de dados no longo prazo (NIST, 2024).

O NIST também enfatiza a importância de uma transição precoce para esses padrões, pois a implementação e a adaptação de novas infraestruturas de segurança são processos complexos e demorados. Empresas, organizações governamentais e

setores sensíveis, como o de saúde e financeiro, são encorajados a iniciar a adoção dos padrões FIPS 203, 204 e 205 para fortalecer a segurança contra ameaças futuras. A inclusão de instruções técnicas detalhadas nos novos FIPS visa facilitar essa integração em sistemas existentes, adaptando-se às especificidades de cada ambiente de uso (NIST, 2024).

Segunda Rodada de Avaliação de Algoritmos de Assinatura Digital PósQuântica pelo NIST

O Instituto Nacional de Padrões e Tecnologia (NIST) anunciou, em outubro de 2024, o avanço de 14 algoritmos de assinatura digital para a segunda rodada do processo de padronização de criptografia pós-quântica, atualmente em fase de testes. Esses algoritmos foram selecionados com base na resistência demonstrada contra potenciais ataques quânticos e pela robustez em diversos cenários de aplicação, incluindo dispositivos com capacidades computacionais limitadas, como os de Internet das Coisas (IoT) (NIST, 2024).

Esse processo faz parte do programa de padronização do NIST, iniciado em 2016. A avaliação desses 14 novos algoritmos de assinatura digital representa a expansão do portfólio de segurança pós-quântica do NIST, assegurando que existam múltiplas alternativas de proteção digital, caso novas vulnerabilidades sejam descobertas no futuro (NIST, 2024).

Os 14 algoritmos que avançaram para essa segunda rodada são (NIST, 2024):

- CROSS (NIST, 2024)
- FAEST (NIST, 2024)
- HAWK (NIST, 2024)
- LESS (NIST, 2024)
- MAYO (NIST, 2024)
- MIRATH (NIST, 2024)
- MQOM (NIST, 2024)
- PERK (NIST, 2024)
- QR-UOV (NIST, 2024)
- RYDE (NIST, 2024)

- SDitH (NIST, 2024)
- SNOVA (NIST, 2024)
- SQIsign (NIST, 2024)
- UOV (NIST, 2024)

Durante essa segunda rodada, os desenvolvedores dos algoritmos terão a oportunidade de aprimorar especificações e implementar ajustes necessários para maximizar a segurança e eficiência. O NIST conduzirá uma revisão técnica aprofundada de cada algoritmo em ambientes de teste variados, com um período estimado de avaliação de 12 a 18 meses. Esses testes incluem a análise do desempenho dos algoritmos em sistemas de TI de alta capacidade, dispositivos móveis e plataformas de IoT, buscando garantir que possam ser implementados em uma variedade de contextos com demandas de segurança distintas (NIST, 2024). O objetivo é garantir que os algoritmos de assinatura digital não apenas sejam resistentes a ataques de computadores quânticos, mas também práticos para implementação em dispositivos de pequeno porte, que possuem limitações de energia e processamento (NIST, 2024).
Essa abordagem é fundamental para proteger infraestruturas críticas, como sistemas financeiros e governamentais, além de promover segurança em dispositivos de uso pessoal e comercial (NIST, 2024).

O FUTURO DA INTERNET QUÂNTICA

O futuro da Internet Quântica é promissor e repleto de possibilidades positiva, com o potencial de revolucionar diversos setores da sociedade. Apesar de ainda estar em fase de pesquisa e desenvolvimento, o investimento e dedicação a esta tecnologia só cresce.

Com a aplicação da Internet Quântica para a sociedade, precisa ter atenção nos seguintes impactos que ela irá trazer:

Segurança aprimorada: a criptografia quântica tornou praticamente impossível intercepção ou espionagem de dado.

Velocidade aumentada: a Internet Quântica poderá transmitir informações muito mais rápido que a Internet convencional.

Maior eficiência e Infraestrutura própria: a Internet Quântica pode resolver problemas mais complexos com mais eficiência e agilidade que os computadores convencionai, mas para seu funcionamento, é necessário ter uma infraestrutura adequada para suportar esta tecnologia.

Impacto na sociedade: a aplicação da Internet Quântica na sociedade para acarretar grandes impactos (negativos ou positivo) para a sociedade que já está acostumada com a Internet convencional. E sua migração pode ser bem aceita, como também pode ser difícil de ser aceita.

REFERÊNCIAS

BROSSO, I. “Computação Quântica: “A realidade de uma nova era”, ed. Altas Books, 2020.

https://bit.ly/3WmrlxF

BRUMATTO, H. “Introdução à Computação Quântica”, Unicamp, 2010.

SILVA, W. “Introdução à Computação Quântica”, IME-USP, 2018.

ESTEFANSKI, J. “O que é emaranhamento quântico? Tudo sobre essa peculiaridade ‘assustadora’ da física”, Universo Cético, 2022.

https://universocetico.com/o-que-e-emaranhamento-quantico-tudo-sobre-essapeculiaridade-assustadora-da-fisica/

REIS, F. “O que é um Computador Quântico - Conceitos e Funcionamento”, Bóson Treinamentos, 2020.

https://youtu.be/s9MyPVujd7E

LOOS, P. “O que vai acontecer no FIM da Lei de Moore?”Ciência Todo Dia, 2021. https://youtu.be/35XqzsGcQRk

PHYS “Quantum loop: US unveils blueprint for 'virtually unhackable' internet”, Phys.org, 2020 https://phys.org/news/2020-07-quantum-loop-unveils-blueprint-virtually.html PORTAL GOV: Ministério da Ciência, Tecnologia e Inovação https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/08/cientistasapresentam-possibilidades-para-desenvolver-a-computacao-e-internet-quantica-nobrasil

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - Quantum Computing and Communication; Paul E. Black, D. Richard Kuhn, Carl J. Williams https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51022

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. 23 ago. 2023. Disponível em: https://www.nist.gov/news-events/news/2023/08/niststandardize-encryption-a lgorithms-can-resist-attack-quantum-computers. Acesso em: 18 nov. 2024.

IBM. What is Quantum Cryptography?. Disponível em: https://www.ibm.com/brpt/topics/quantum-cryptography. Acesso em: 18 nov. 2024.

ID QUANTIQUE. Quantum Safe Security. Disponível em: https://www.idquantique.com/. Acesso em: 18 nov. 2024.

GOOGLE QUANTUM AI. Our mission. Disponível em: https://quantumai.google/. Acesso em: 18 nov. 2024.

QUANTUM FLAGSHIP. Quantum technologies for Europe. Disponível em: https://qt.eu/. Acesso em: 18 nov. 2024.

TOSHIBA. Quantum Key Distribution (QKD). Disponível em: https://www.toshiba.eu/pages/en/quantum-key-distribution/. Acesso em: 18 nov. 2024.

QUANTUM INSIDER. Quantum Computing Companies: A Full 2024 ListQuantum Computing Companies: A Full 2024 List (thequantuminsider.com) Acesso em: 18 nov. 2024

FORBES. Top 10 Quantum Computing Companies Making Top 10 Quantum Computing Companies Making Change (forbes.com). Acesso em: 18 nov. 2024