Computação Quântica

Para Administradores de Rede

ou

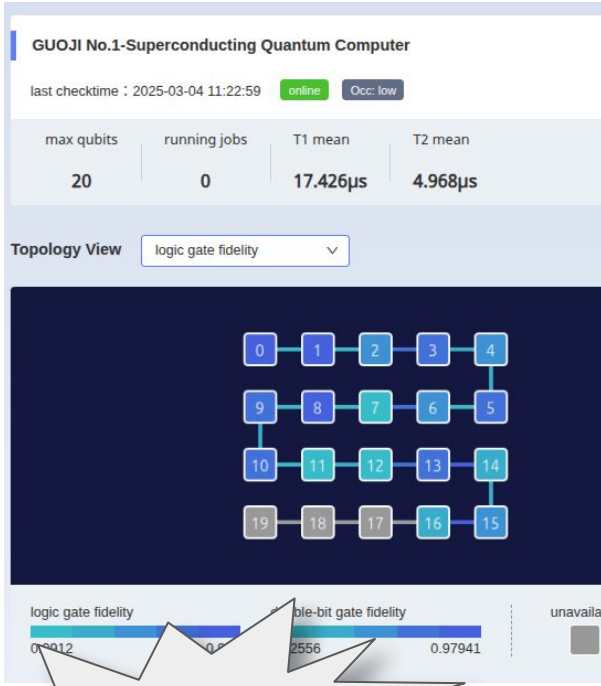
Schrödinger estava certo e errado ao mesmo tempo

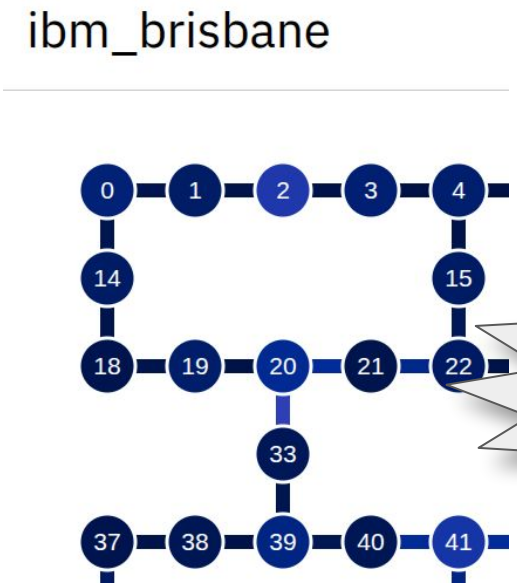
Jessian Ferreira Cavalcanti <jessian@nic.br>

1 0

10 pontos a esclarecer

- Conceitos de Computação Quântica
- Mitos e Verdades
- Exemplos de algoritmos
- Chaves criptográficas
- Vulnerabilidades
- O que não podemos evitar
- O que podemos evitar
- Criptografia Pós-quântica
- OpenSSL 3.5
- Equipamentos

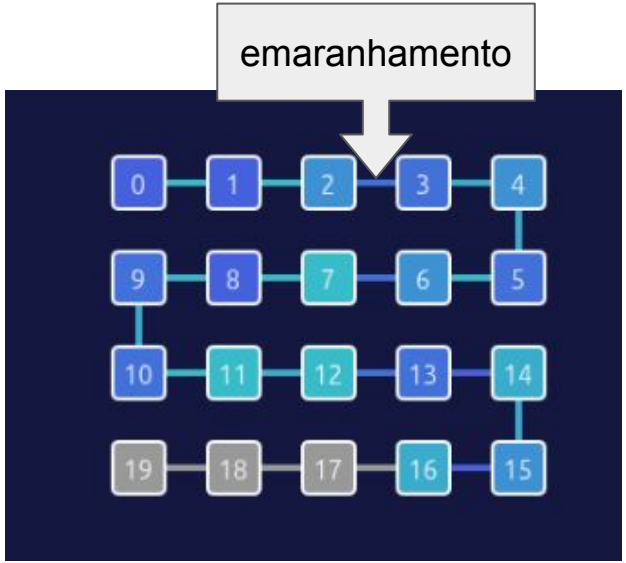




Imagens raras !!

Conceitos

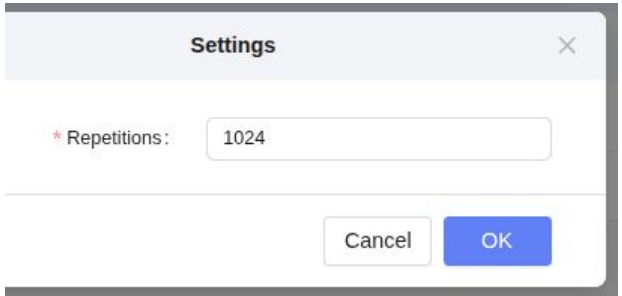
- Circuitos com comportamento quântico
  - Superposição: previsibilidade estatística
  - Emaranhamento: qubits que se entrelaçam
- Desafio de Engenharia
  - Oscilador em supercondutor
  - Qubits ópticos
  - Mitigação de ruídos
- Composição com computador clássico
  - Envio de código a ser rodado (cloud)
  - Leitura do resultado
  - Laços e eventual retro-alimentação de resultados



Mitos e Verdades

- Entendendo a Superposição com o exemplo do “gato de Schrödinger”
  - Trata-se de uma imagem criada para exercício mental mas tem sido utilizada erradamente
  - Superposição visa consolidar a estatística envolvida nos fenômenos quânticos
- Velocidade de processamento: vantagens e desvantagens (lento comparado à rede?)
- Qubits físicos x Qubits lógicos
- Emaranhamento com partículas externas ao experimento (futurologia)
- Resultado calculado com uma rajada de eventos (*shots*)

```
# Construct the Estimator instance.

estimator = Estimator(mode=backend)
estimator.options.resilience_level = 1
estimator.options.default_shots = 1000
```

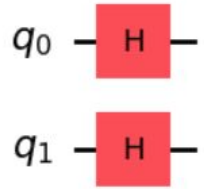


Exemplos

- Gerador de Números Aleatórios
  - Utilizando Qiskit

```python
from qiskit import QuantumCircuit

# Create a new circuit with two qubits
qc = QuantumCircuit(2)
qc.h([0,1])
# qc.h(0)
qc.draw("mpl")
```

[2] ✓ 0.7s Python



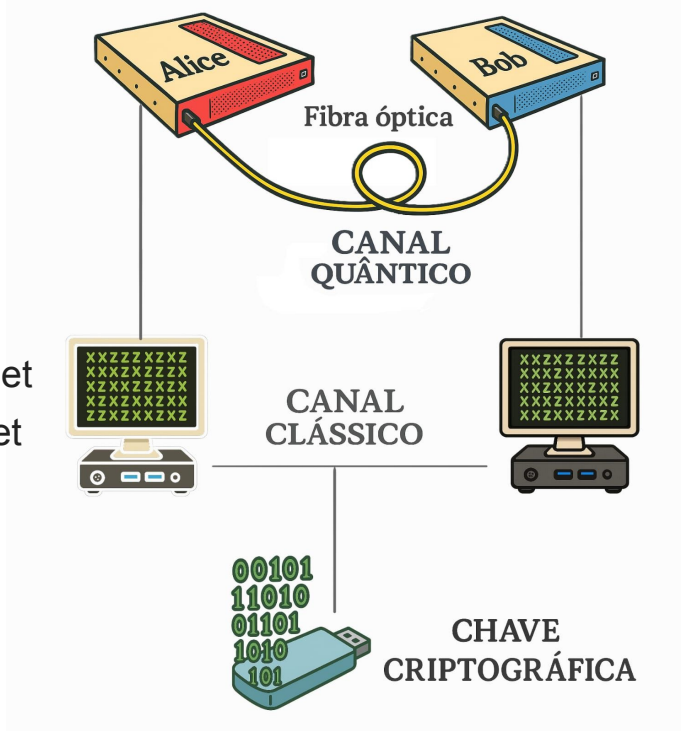

```python
from qiskit.quantum_info import Statevector

psi = Statevector(qc)
psi.draw("latex")
```

[3] ✓ 0.5s Python

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

Chaves Criptográficas

- Quantum Key Distribution (2014)
- Sequência perfeitamente aleatória
- Segurança na transmissão
- Quantum Internet Research Group:
  - **RFC 9583** Application Scenarios for the Quantum Internet
  - **RFC 9340** Architectural Principles for a Quantum Internet



https://www.ime.eb.mil.br/home/noticias/ime-internet-quantica-no-brasil

Vulnerabilidades

- Chave RSA pode ser decodificada pelo algoritmo de Shor
  - Foi desenvolvido antes mesmo do primeiro hardware quântico
- Exemplo: Etapas iniciais do HTTPS
- e outros

O que não podemos evitar

- Pacotes capturados e guardados para posterior decodificação
  - *Harvest now, decrypt later*
- Computador Quântico em mãos erradas
- Atualizar o HTTPS

O que podemos evitar

- Novas capturas que possam ser descriptografadas
- HTTPS vulnerável
- Certificado com mais de 45 dias

Criptografia Pós-quântica

- **RFC 8784** Mixing Preshared Keys in the [...] (IKEv2) for Post-quantum Security
- **RFC 9370** Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- **RFC 9794** Terminology for Post-Quantum Traditional Hybrid Schemes
- Internet Draft
  - https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/
- Como funciona
  - Algoritmos invulneráveis a processamento em computador quântico
- Onde está implantada
  - Navegadores
  - OpenSSL 3.5

OpenSSL 3.5

- Disponível no Ubuntu 25.10
- Como utilizar no Python
- Como utilizar via Docker
  - docker run alpine/openssl:3.5.2 list -kem-algorithms

```
  { 1.2.840.113549.1.1.1, 2.5.8.1.1, RSA, rsaEncryption } @ default
  { 1.2.840.10045.2.1, EC, id-ecPublicKey } @ default
  { 1.3.101.110, X25519 } @ default
  { 1.3.101.111, X448 } @ default
  { 2.16.840.1.101.3.4.4.1, id-alg-ml-kem-512, ML-KEM-512, MLKEM512 } @ default
  { 2.16.840.1.101.3.4.4.2, id-alg-ml-kem-768, ML-KEM-768, MLKEM768 } @ default
  { 2.16.840.1.101.3.4.4.3, id-alg-ml-kem-1024, ML-KEM-1024, MLKEM1024 } @
default
  X25519MLKEM768 @ default
  X448MLKEM1024 @ default
  SecP256r1MLKEM768 @ default
  SecP384r1MLKEM1024 @ default
```

Dispositivos e Equipamentos

- Roteador quântico
  - Iniciativa recente do IME-RJ
  - Equipamentos certificados ao longo do canal de distribuição para prolongar distâncias
  - Entra na Topologia da Internet Quântica
- Computador quântico
  - CBPF e UFCG
  - Muitas empresas oferecem o produto pronto
  - Ou somente o equipamento de resfriamento
  - Versões didáticas

spinquanta.com

Ivan S. Oliveira e João Paulo Sinnecker - Crédito: NCS/CBPF

https://www.gov.br/cbpf/pt-br/assuntos/noticias/2025-o-ano-da-quantica-e-o-papel-do-cbpf-no-brasil