O maior evento de Segurança
da Informação e Cyber Security
da América Latina

mind the sec /2023

MAIS UM EVENTO Flipside

REALIZAÇÃO Green Helmet

mind the sec /2023

Segurança Cibernética na Era Quântica

Disclaimer

- Total autorresponsabilidade
- Pesquisa independente (“um pouco” de coragem)
- *Insights*: sem dogmas, sem previsões
- Objetivo geral : encontrar/provocar pessoas mais habilidosas, capacitadas e interessadas no tema
- Objetivo específico: trabalharmos juntos

Bio

/jullyanolino

Graduação em Ciência da Computação (UFPI)

Licenciatura em Matemática (IESB)

Pós-graduação em Computação Quântica (UniRitter)

CISSP
C|TIA

Analista de Segurança Cibernética (ENAP)

Pesquisador em *Quantum Internet & Cybersecurity* (Ânima Lab)

Artigo: "*Sensoriamento remoto quântico aplicado na Defesa Nacional*" (I Encontro Nacional de Tecnologias Quânticas para Defesa - ITA)

Agenda

mind the sec /2023

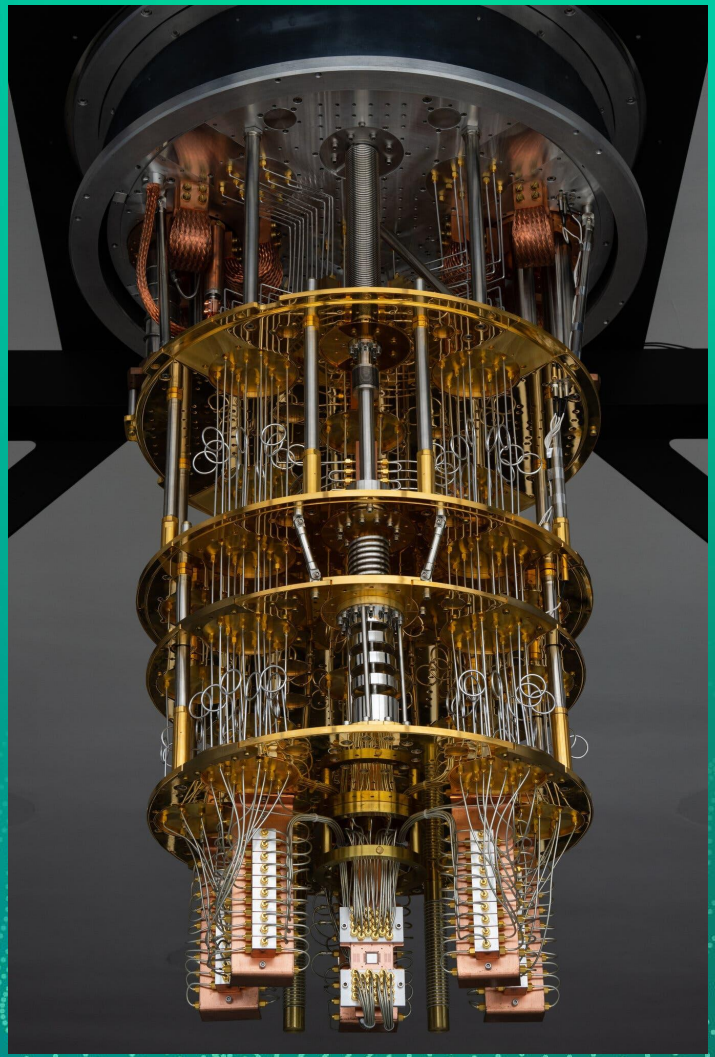
Fundamentos

Riscos de Segurança

Soluções & Oportunidades

"I think I can safely say that nobody understands quantum mechanics"

(Richard Feynman)



With just 275 qubits, we can represent more states than the number of atoms in the observable universe

$$2^{275}$$

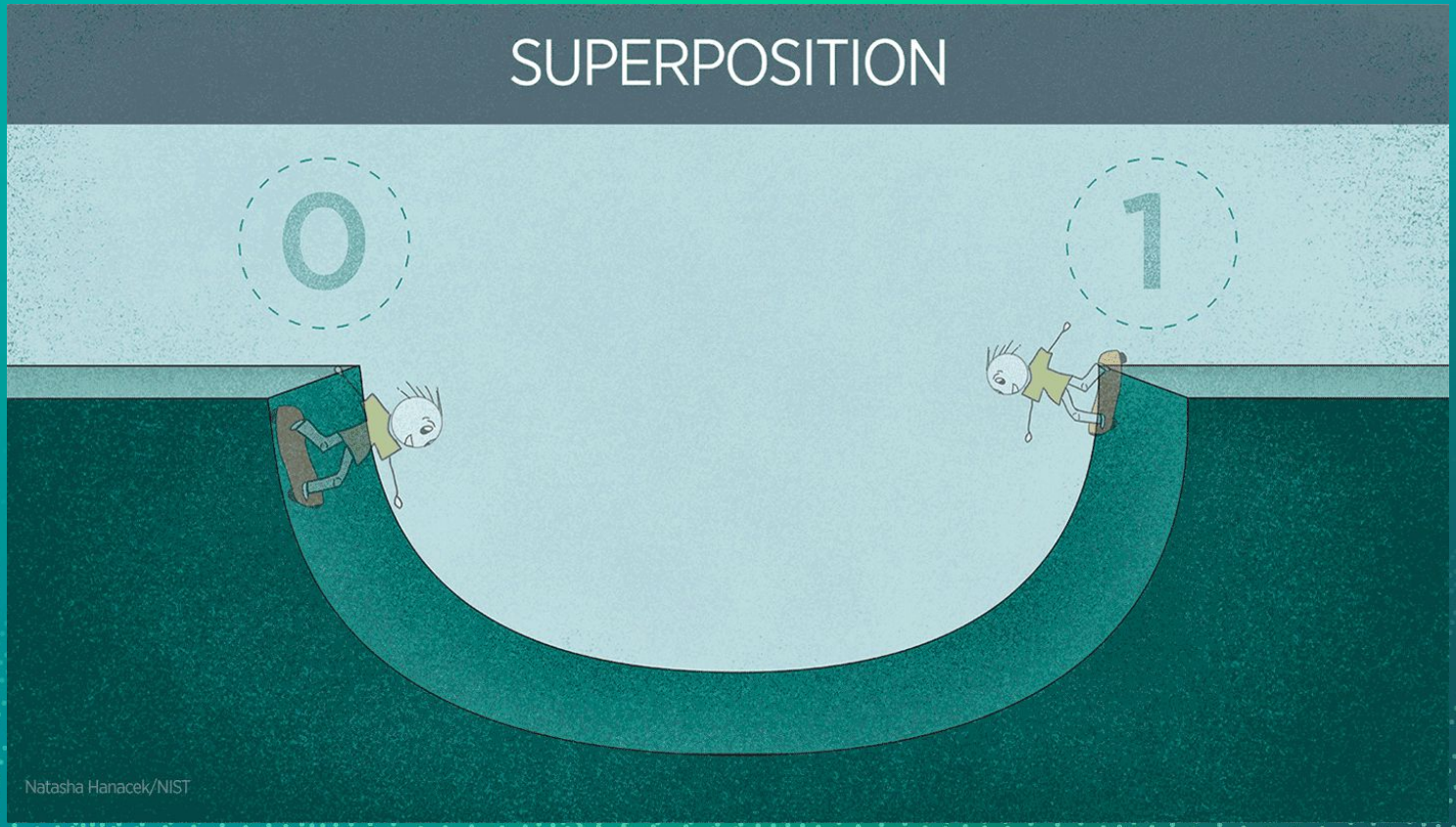
Fundamentos

Superposição

Emaranhamento

Interferência

paralelismo & exponencialidade



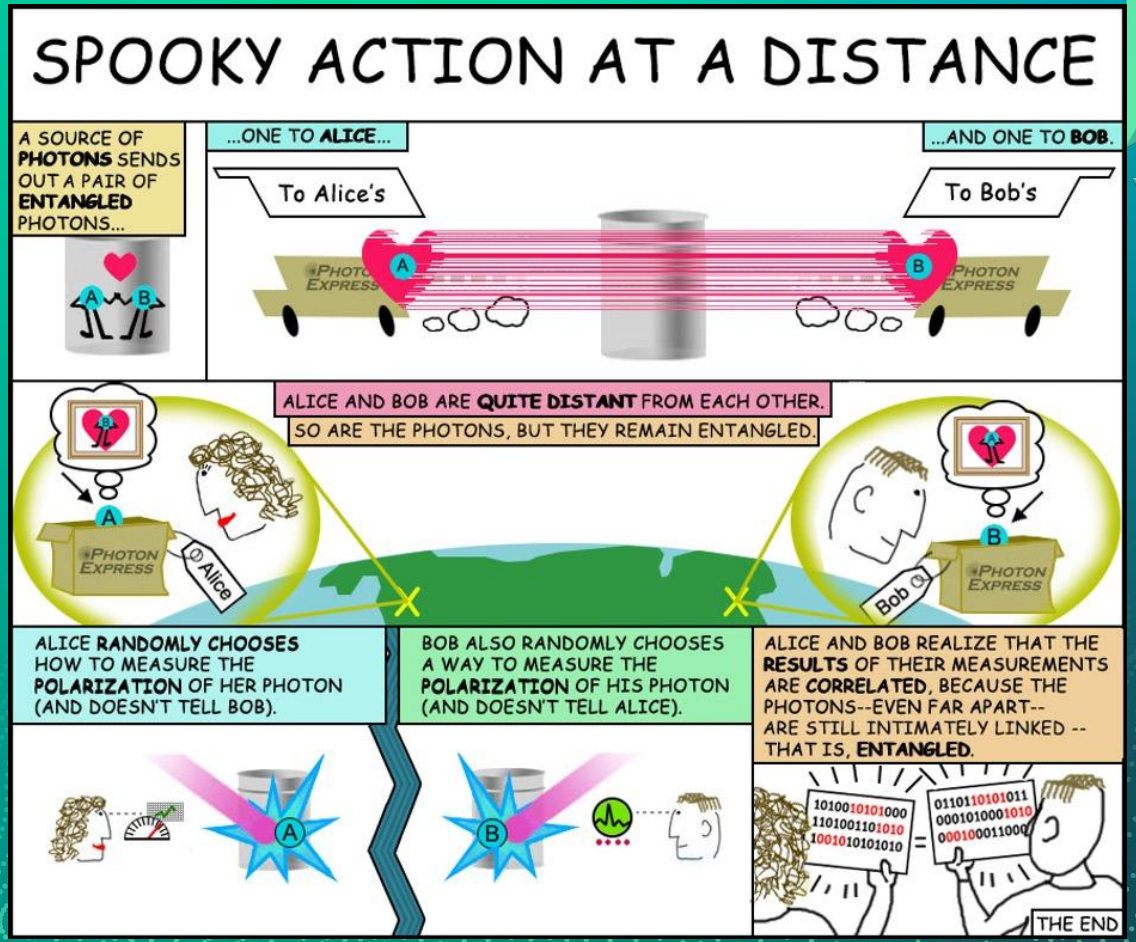
mind the sec /2023

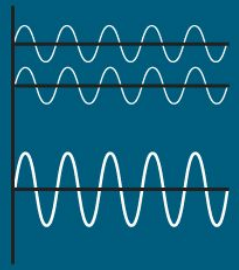
\+

Informação

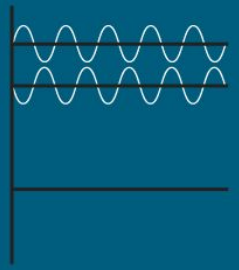
↑

Comunicação





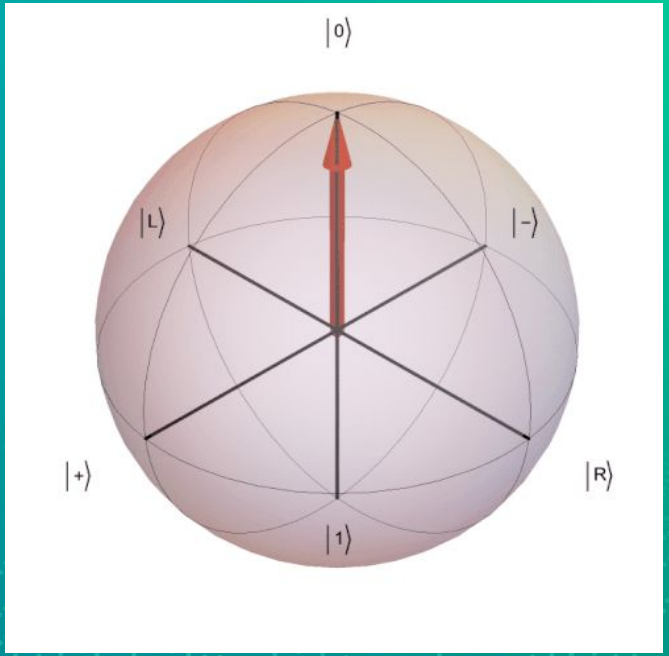
CONSTRUCTIVE
INTERFERENCE

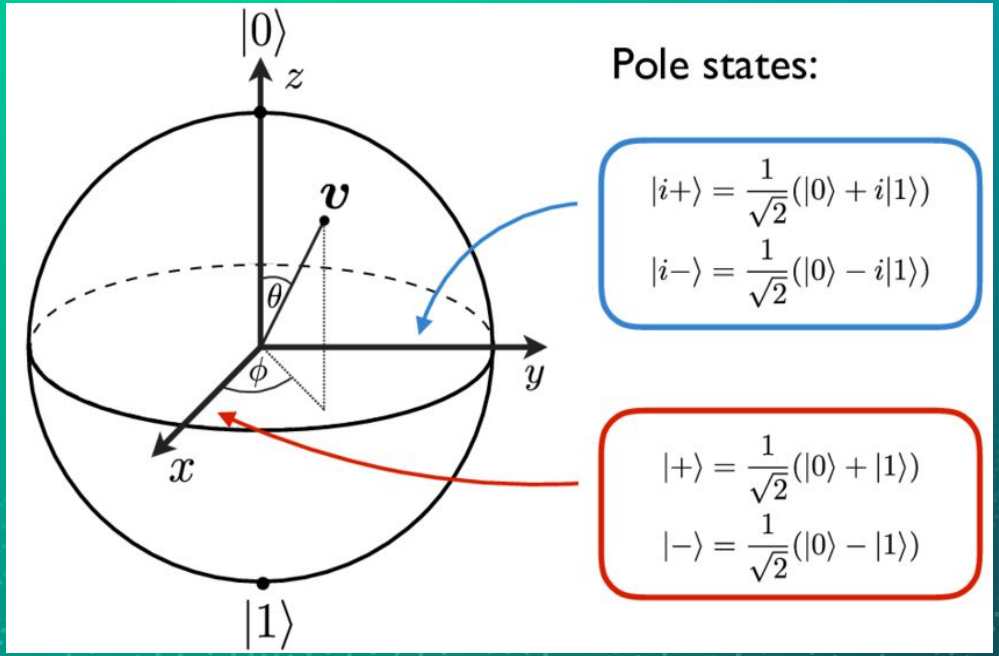


DESTRUCTIVE
INTERFERENCE

Cancelamento de Ruído

Qubit


|0⟩
|L⟩
|-⟩
|+⟩
|R⟩
|1⟩


|0⟩
z
v
θ
y
ϕ
x
|1⟩
Pole states:
$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$
$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

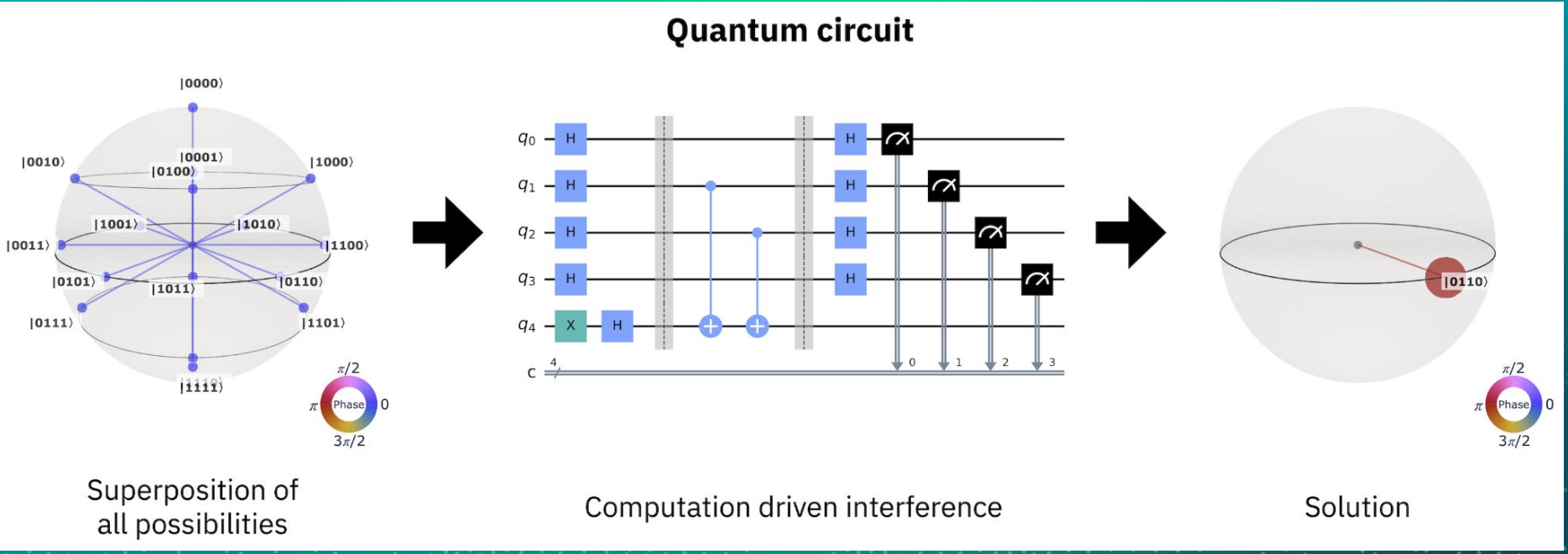
Tecnologias

Supercondutores

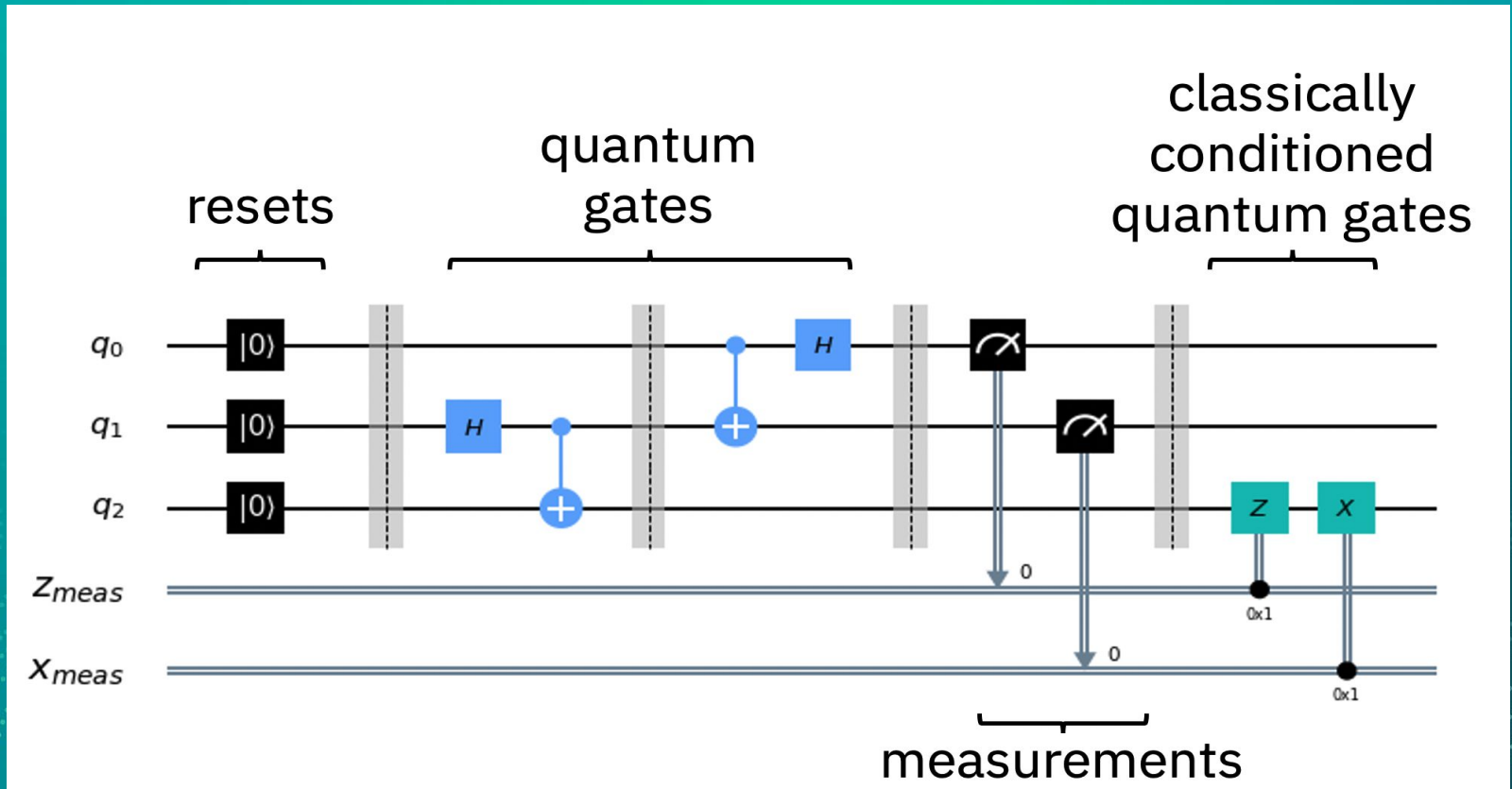
Trapped Ions

Spin qubits

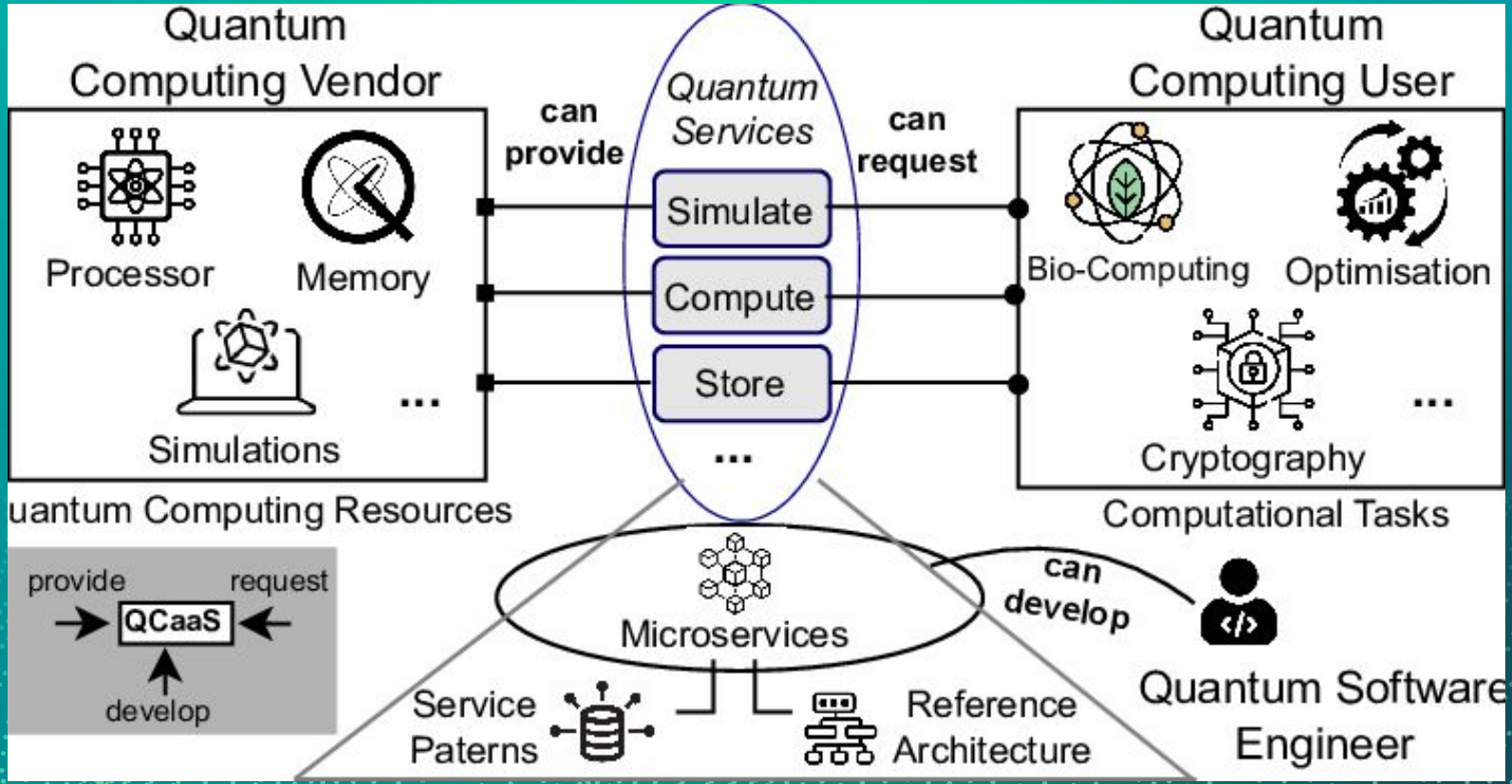
Modelo


Quantum circuit
|0000⟩
|0010⟩
|0001⟩
|0100⟩
|1000⟩
|1001⟩
|1010⟩
|0011⟩
|1100⟩
|0101⟩
|1011⟩
|0110⟩
|0111⟩
|1101⟩
|1111⟩
π/2
π
Phase
0
3π/2
q_0
q_1
q_2
q_3
q_4
c
H
X
0
1
2
3
|0110⟩
Superposition of all possibilities
Computation driven interference
Solution

Algoritmos & Protocolos



“QCaaS”


Quantum
Computing Vendor
Processor
Memory
Simulations
...
uantum Computing Resources
can
provide
Quantum
Services
Simulate
Compute
Store
...
can
request
Quantum
Computing User
Bio-Computing
Optimisation
Cryptography
...
Computational Tasks
provide
request
QCaaS
develop
Microservices
can
develop
Service
Paterns
Reference
Architecture
Quantum Software
Engineer

Empresas

Honeywell International
Intel Corporation
IBM Corporation
NVIDIA Corporation
Amazon
Alphabet Inc.
Microsoft Corporation

Xanadu, ColdQuanta, QC Ware

Rigetti Computing, Inc.
D-Wave Quantum Inc.
Quantum Corporation
IonQ, Inc.
Atos SE
Toshiba Corporation
Baidu, Inc.
Alibaba

Quantum SDK

Quantum Computing Programming Languages

QUANTUM WORLD ASSOCIATION

Quantum Universal Languages	XACC						
	ProjectQ				CirqProjectQ		
	IBM	**Rigetti**	**DWave**	**Xanadu**	**Google**	**Microsoft***	**Qilimanjaro***
Full-stack libraries	QISKit	Forest		Strawberry Fields	Cirq	Quantum Development Kit	
Quantum algorithms	QISKit Aqua	Grove	QSage ToQ		OpenFermion -Cirq	Q#	
Quantum circuits	QISKit Terra	pyquil	qbsolv		Cirq		Qibo
Assembly language	Open QASM	Quil	QMASM	Blackbird	Other Quantum Machine Instruction Languages		
Hardware	Quantum device						

* Hardware under development. Quantum programs are run on their own simulators.

"Quantum Language" is refered with no distinction both as a quantum equivalence of a programming language and as a library to write quantum programs supported by some well-known classical programming language.

mind the sec /2023

Aplicações

Quantum Machine Learning

Quantum Finance

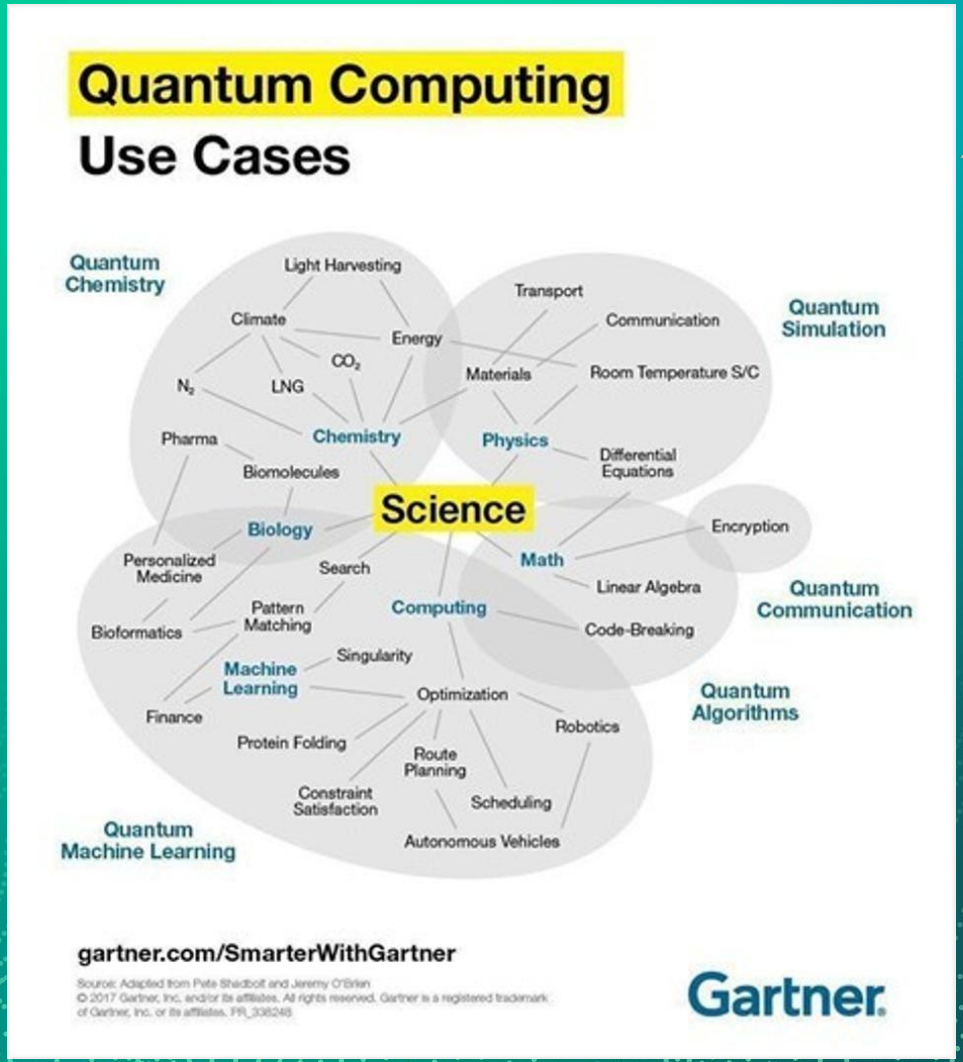
Quantum Optimization

Quantum Chemistry

Quantum Imaging & Sensing

Saúde
Mercado financeiro
Comércio
Comunicações
Energia
Exploração espacial
Defesa nacional

Segurança Cibernética



Desafios

ruído e decoerência

escalabilidade

correção de erro

algoritmos eficientes

interface quântica e clássica

vantagens computacionais

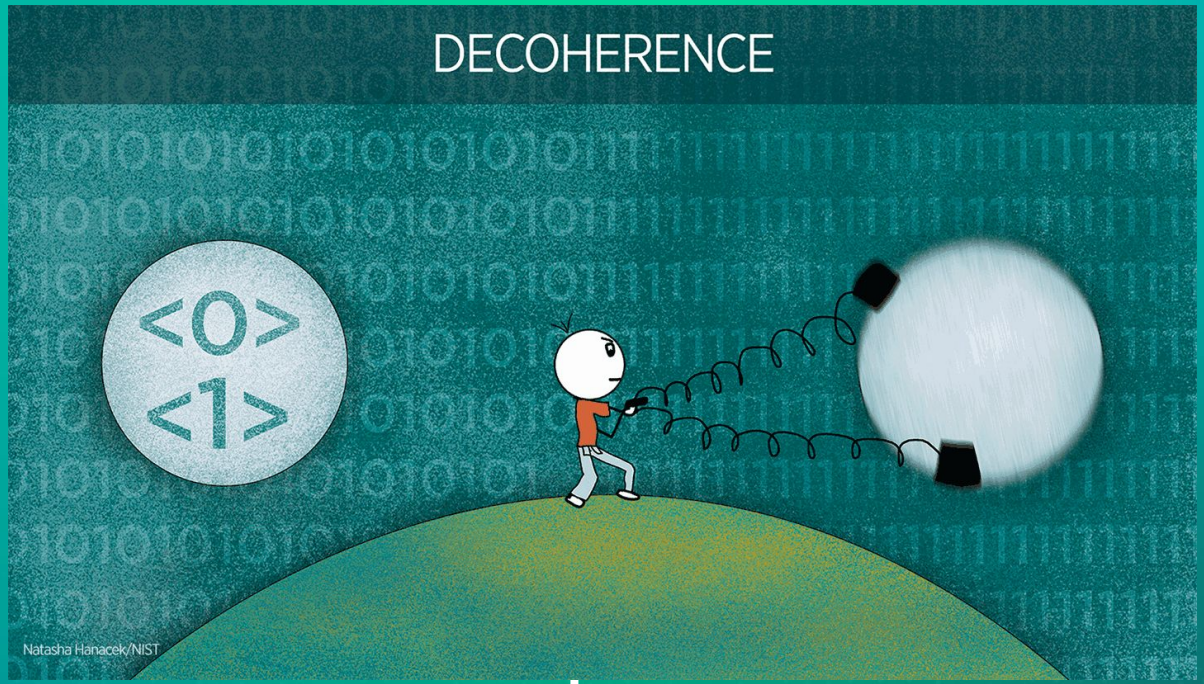
padrões e protocolos

mapeamento de problemas

benchmarking

talentos

natureza linear & problemas não-lineares



NISQ

(“*noisy intermediate scale quantum*”)

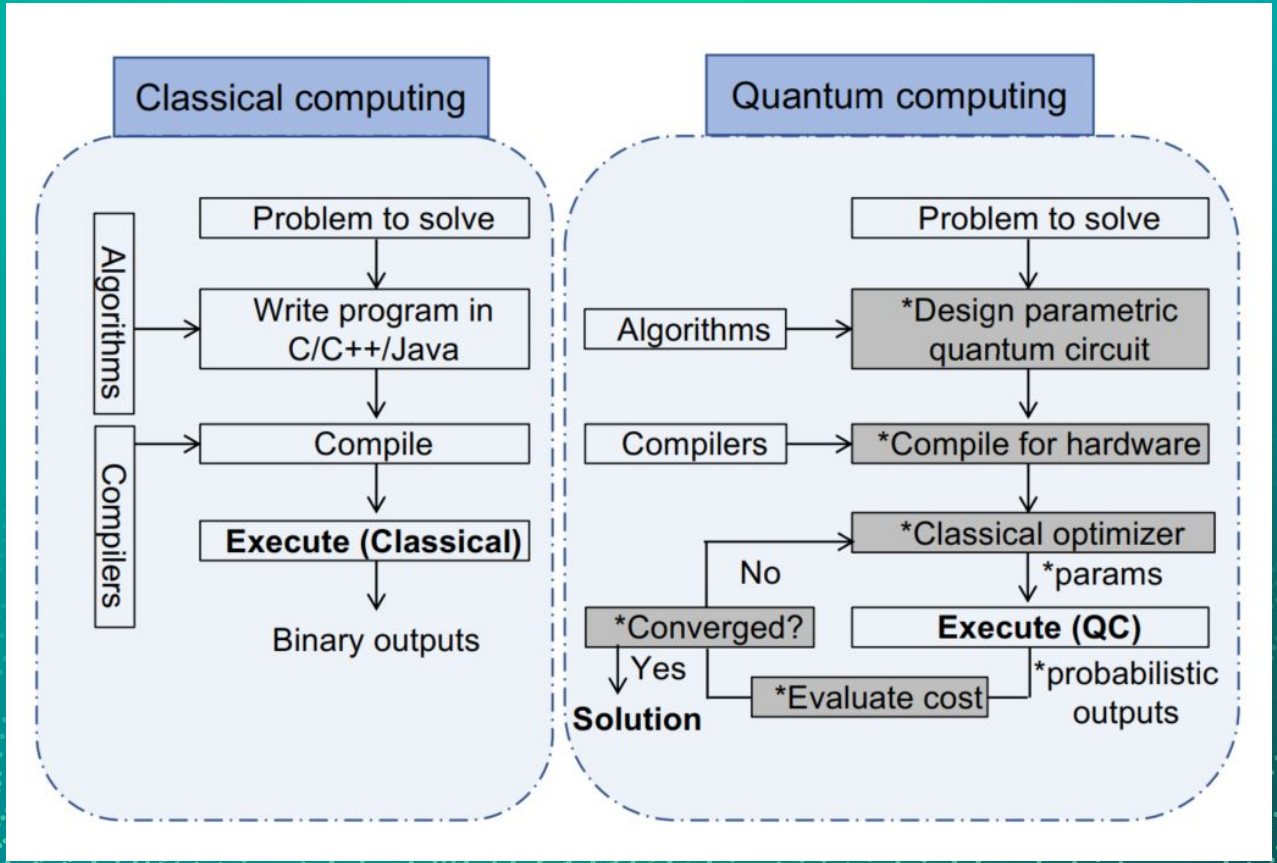
Riscos

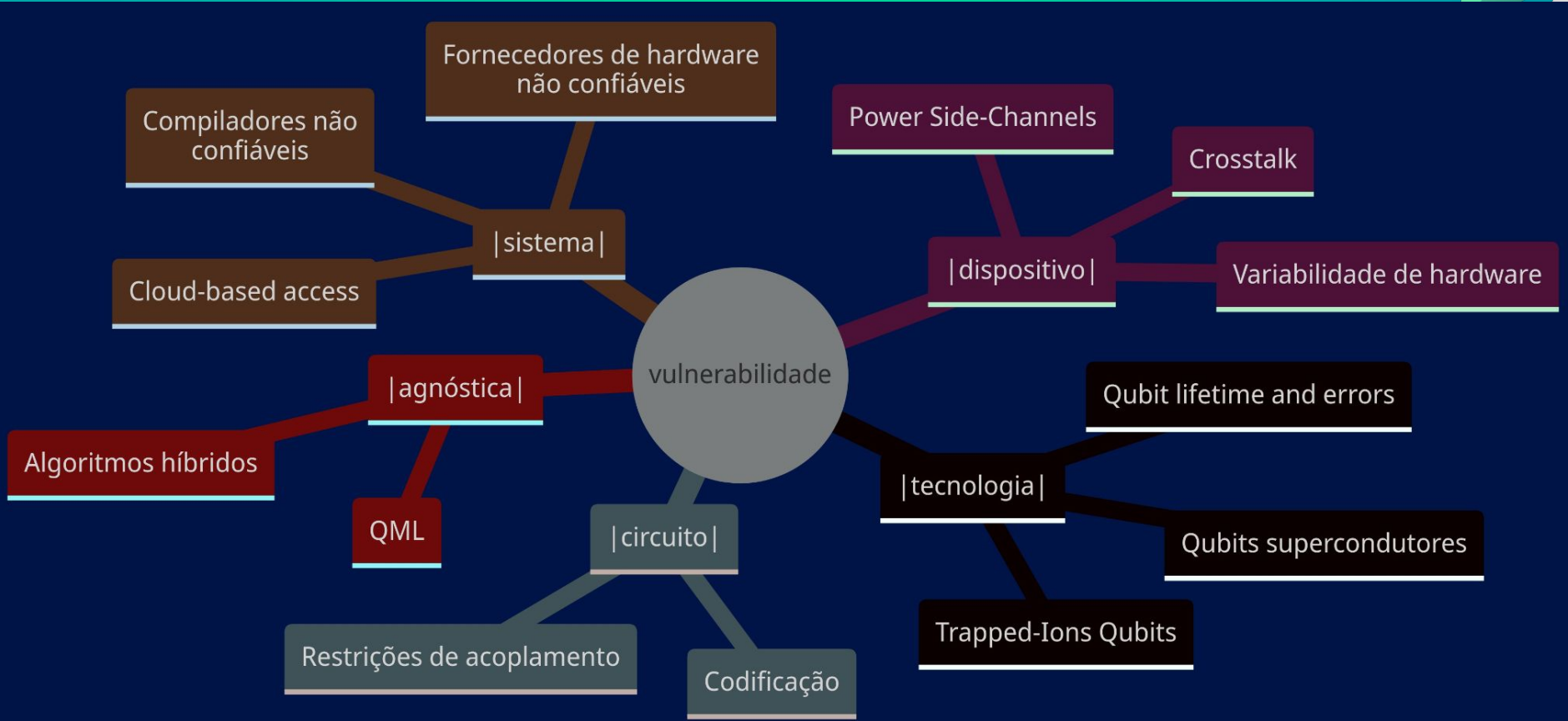
Ameaças

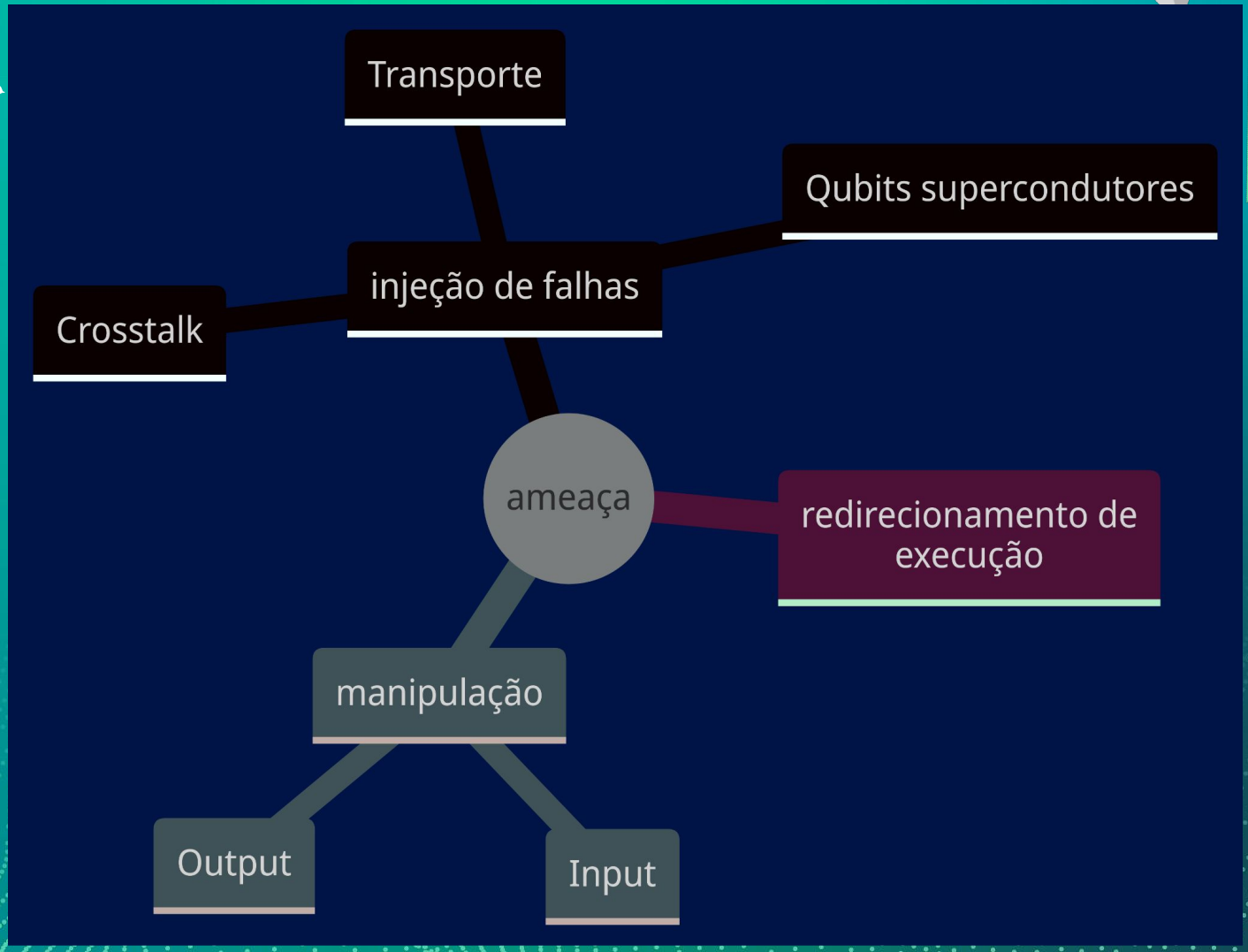
Vulnerabilidades

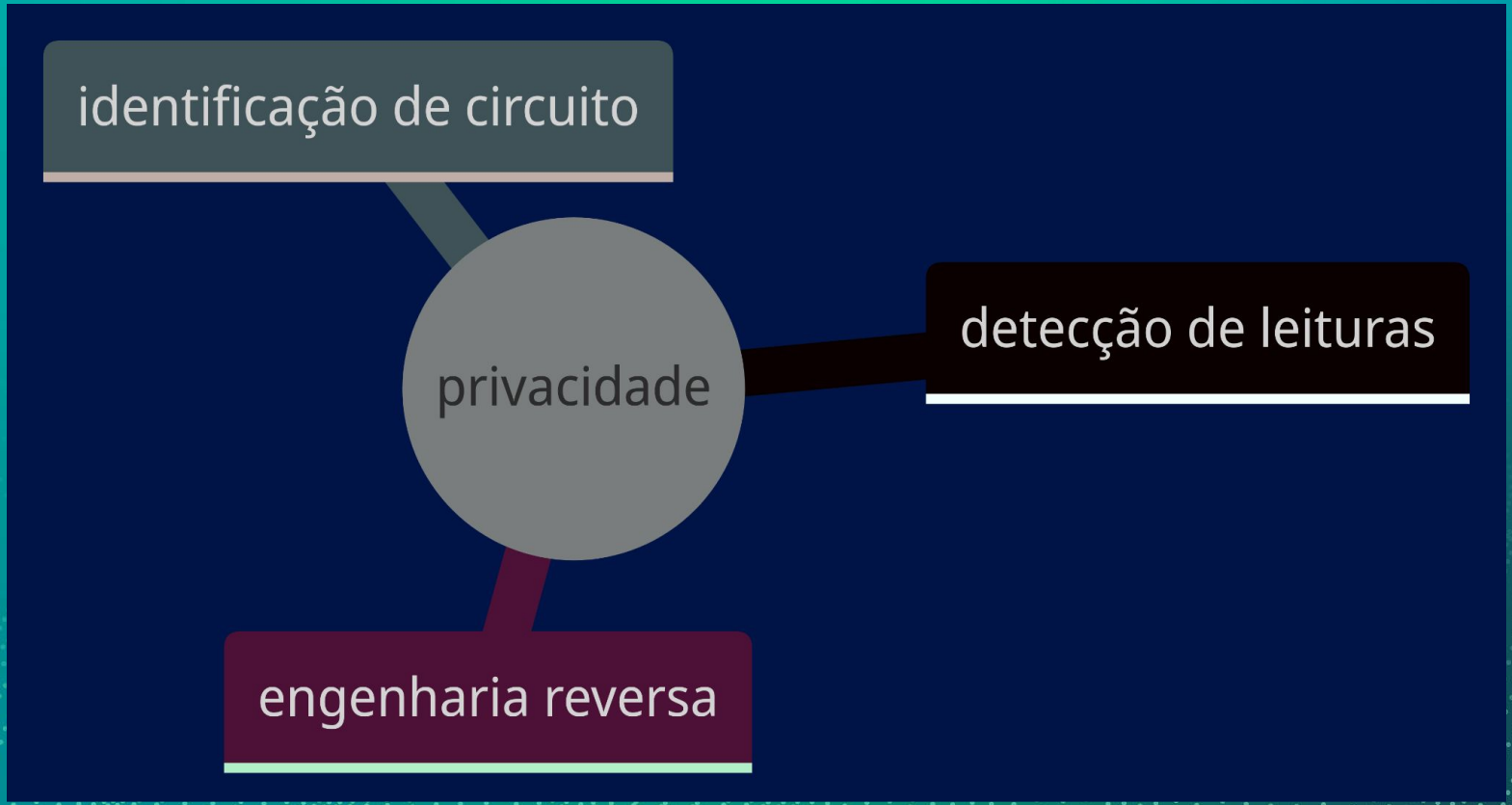
Privacidade

Revisão dos Paradigmas




Fornecedores de hardware não confiáveis
Compiladores não confiáveis
|sistema|
Cloud-based access
Power Side-Channels
Crosstalk
|dispositivo|
Variabilidade de hardware
vulnerabilidade
|agnóstica|
Algoritmos híbridos
QML
|circuito|
Restrições de acoplamento
Codificação
Qubit lifetime and errors
|tecnologia|
Qubits supercondutores
Trapped-Ions Qubits


Transporte
Qubits supercondutores
injeção de falhas
Crosstalk
ameaça
redirecionamento de execução
manipulação
Output
Input


identificação de circuito
privacidade
detecção de leituras
engenharia reversa

Resultados

Soluções

Oportunidades

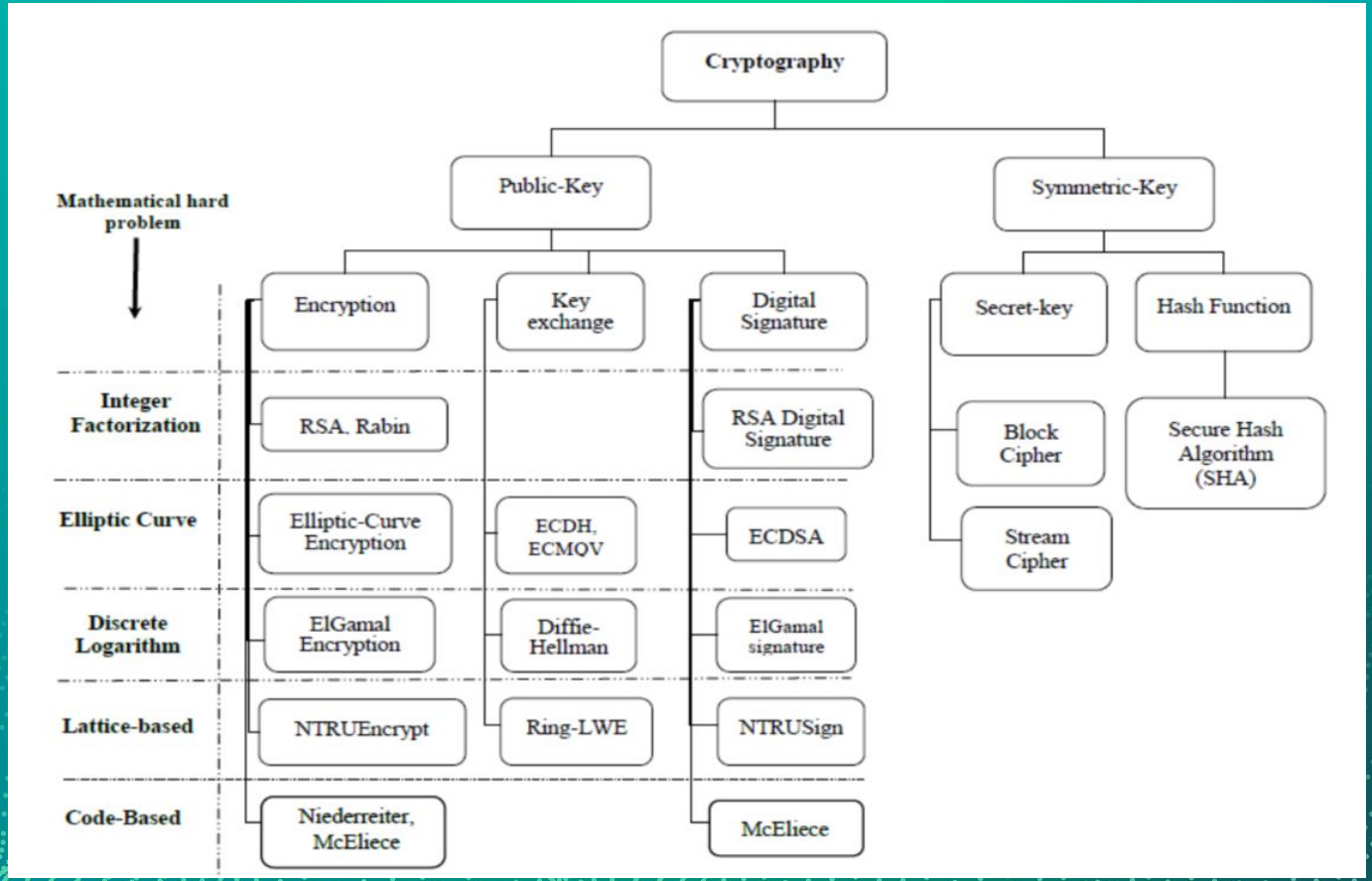
Discussões

SOLUÇÕES


MECANISMOS DE DEFESA
QUANTUM ANTIVIRUS
ISOLAMENTO CONTRA CROSSTALK
COMPILAÇÃO PARTICIONADA
RASTREAMENTO DE MUDANÇAS EM TAXAS DE ERROS
OBFUSCAÇÃO
QUANTUM PHYSICAL UNCLONABLE FUNCTIONS (QUPUF)
BLINDING
PROTEÇÃO AOS CIRCUITOS

mind the sec /2023

Post-Quantum Cryptography (PQC)
X
Quantum Cryptography


Cryptography
Public-Key
Symmetric-Key
Mathematical hard problem
Encryption
Key exchange
Digital Signature
Secret-key
Hash Function
Integer Factorization
RSA, Rabin
RSA Digital Signature
Block Cipher
Secure Hash Algorithm (SHA)
Elliptic Curve
Elliptic-Curve Encryption
ECDH, ECMQV
ECDSA
Stream Cipher
Discrete Logarithm
ElGamal Encryption
Diffie-Hellman
ElGamal signature
Lattice-based
NTRUEncrypt
Ring-LWE
NTRUSign
Code-Based
Niederreiter, McEliece
McEliece

Abordagens criptográficas pós-quânticas

Lattice-based cryptography

Multivariate cryptography

Hash-based cryptography

Code-based cryptography

Isogeny-based cryptography

Symmetric key quantum resistance

Abordagens criptográficas quânticas

QKD

Mistrustful quantum cryptography

Noisy-quantum-storage model

Position-based quantum cryptography

Device-independent quantum cryptography

Oportunidades

Supply chain

Tecnologia de qubits

Hardware

Pilha de software

Algoritmos & Protocolos

Cyberforensics

HUMINT

Conscientização

mind the sec /2023

Post-Quantum Cryptography Standardization, Initiative & Agenda

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

EPC
EUROPEAN POLICY CENTRE

Regulamentação e Pesquisa

⟨quantum|gov⟩

ITF
QUANTUM INTERNET
TASK FORCE

mind the sec /2023

Jullyano Lino
jullyanolino[at]gmail[dot]com
(61) **9.8575.0520**
in /jullyanolino

Q&A

mind the sec /2023

Disposto a descobrirmos, juntos, as respostas.