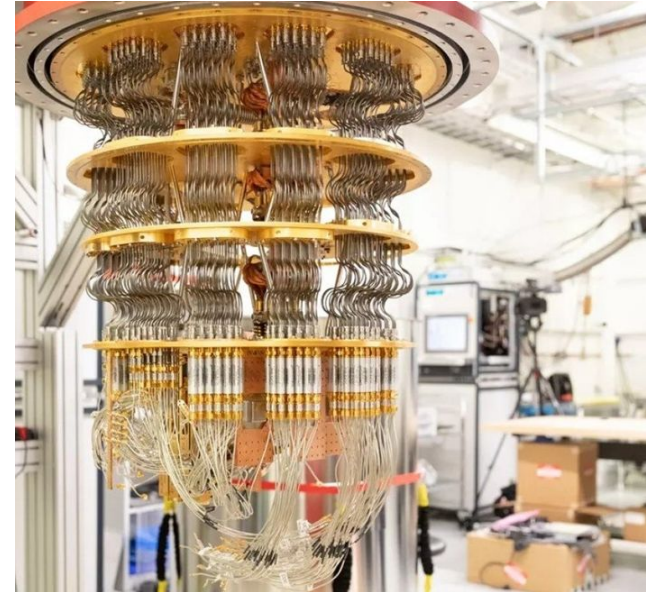


# Minicurso 3 - Introdução à Computação Quântica e Impactos em Criptografia

**Victor Hayashi** (Poli-USP), Bryan Ferreira (IME-USP), **Reginaldo Arakaki** (Poli-USP), Jonatas Rossetti (Bradesco), Routo Terada (IME-USP), Ever Costa (Inteli), **Wildisley Filho** (Inteli), Giovanna Vieira (Inteli), Luiza Petenazzi (Inteli), Priscila Falcão (Inteli)

# Motivação e Objetivo

- A **computação quântica** é uma tecnologia emergente com potencial para resolver problemas complexos, considerados **intratáveis** pelos computadores clássicos
- Esse potencial representa um risco significativo para a segurança da informação, pois **algoritmos quânticos** podem quebrar parte significativa da criptografia usada atualmente
- A quebra de algoritmos como o **RSA** evidencia a necessidade da criptografia pós-quântica e sua padronização pelo **NIST**
- **Objetivo:** Introduzir os fundamentos da computação quântica, examinar seus impactos na criptografia e apresentar soluções como a criptografia pós-quântica



# Motivação e Objetivo

**CSO**

Home • Security • Chinese researchers break RSA encryption with a quantum computer

by Gyana Swain

## Chinese researchers break RSA encryption with a quantum computer

News  
14 Oct 2024 • 4 mins

Data and Information Security Encryption

The research team, led by Wang Chao from Shanghai University, found that D-Wave's quantum computers can optimize problem-solving in a way that makes it possible to attack encryption methods such as RSA.

[Subscribe To Newsletters](#)

**Forbes**

## Debunking Hype: China Hasn't Broken Encryption With Quantum

By [Craig S. Smith](#), Contributor. ⓘ Craig S. Smith, Eye on AI host and former NY... [Follow Author](#)

Oct 16, 2024, 03:58pm EDT

Share Save Comment 2

Recent headlines have proclaimed that Chinese scientists have hacked "military-grade encryption" using quantum computers, sparking concern and speculation about the future of cybersecurity. The claims, largely stemming from a recent [South China Morning Post article](#) about a Chinese academic paper published in May, was picked up by many more [serious publications](#).

However, a closer examination reveals that while Chinese researchers have made incremental advances in quantum computing, the news reports are a huge overstatement.

"Factoring a 50-bit number using a hybrid quantum-classical approach is a far cry from

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- Introdução à Computação Quântica

## Pausa (30 min)

## Parte 2 (1h30)

- Complexidade de Algoritmos
- Algoritmos Quânticos e seus Impactos
- Criptografia Pós-Quântica
- Oportunidades em Computação Quântica

# Agenda

Parte 1 (1h30)

- **Fundamentos de Segurança e Criptografia**
- Introdução à Computação Quântica

Pausa (30 min)

Parte 2 (1h30)

- Complexidade de Algoritmos
- Algoritmos Quânticos e seus Impactos
- Criptografia Pós-Quântica
- Oportunidades em Computação Quântica

# Fundamentos de Segurança e Criptografia



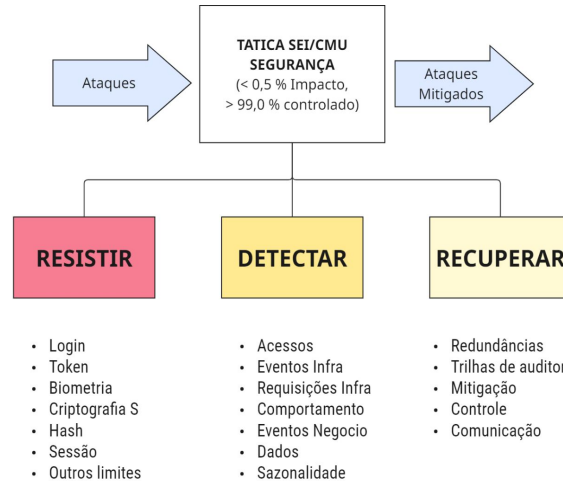
Atributo Arquitetura→

Carnegie Mellon University

Software Engineering Institute

Táticas→

Componentes→



# Fundamentos de Segurança e Criptografia

**Integridade:** proteger contra modificação ou destruição indevida da informação.

**Confidencialidade:** preservar as restrições autorizadas de acesso e divulgação, incluindo mecanismos de proteção da privacidade pessoal e de informações proprietárias.

**Disponibilidade:** assegurar o acesso e uso oportunos e confiáveis da informação.

**Irretratabilidade (não-repúdio)** é a propriedade que um emissor legítimo não possa negar a autoria de uma ação.

**Autenticidade** é a propriedade que garante que uma parte é, de fato, quem afirma ser.



# Fundamentos de Segurança e Criptografia

**Transmissão de Dados:** cenários adversariais possíveis de interceptação, modificação, falsificação, repúdio.

**Dados em Repouso:** cenários adversariais possíveis de acesso indevido, alteração, negação da autoria.

**Processamento:** criptografia homomórfica para privacidade.

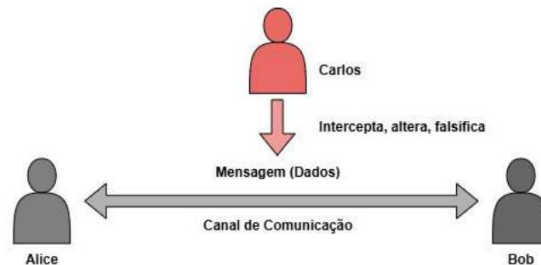


Figura 3.1. Cenário de Transmissão de Dados. Adaptado de [Terada 2008]

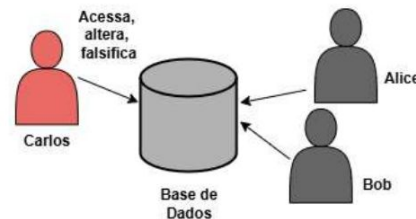


Figura 3.2. Cenário de Dados em Repouso. Adaptado de [Terada 2008]



# Fundamentos de Segurança e Criptografia

## Primitivas Criptográficas

- **Sem Chave:** *keyless hash functions*, PRNG (gerador pseudoaleatório)
- **Simétrica:** mesma chave para cifrar/decifrar (AES)
- **Assimétrica:** par de chaves (RSA, ECC)

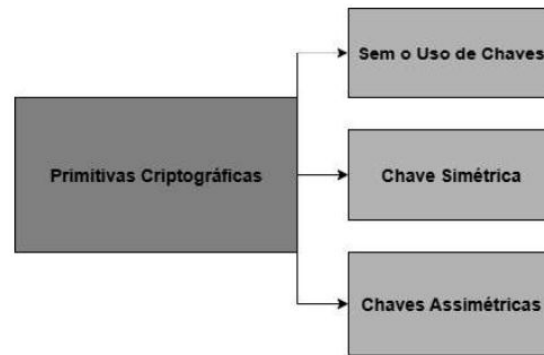
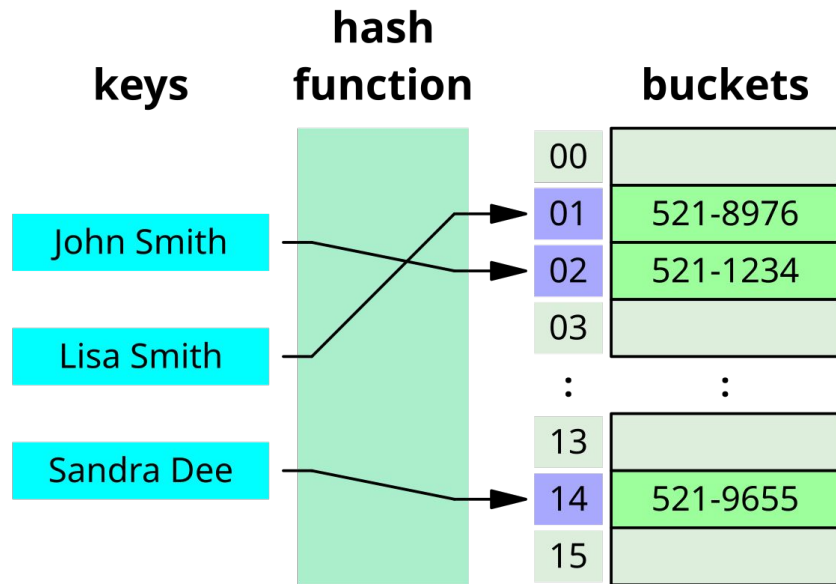


Figura 3.3. Primitivas Criptográficas de Segurança. Adaptado de [Menezes et al. 2018]

# Fundamentos de Segurança e Criptografia

## Funções Hash

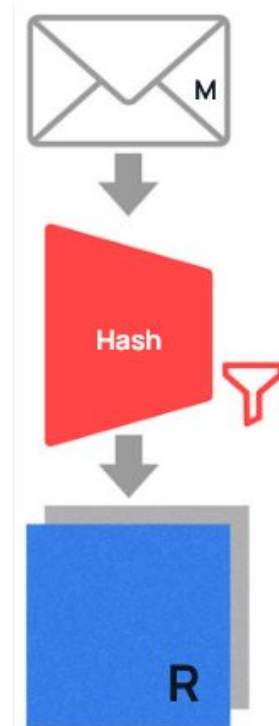
- Originalmente usadas em estruturas de dados (**tabela hash**) para acesso eficiente a informações
- Função hash é **determinística** e produz saída de **comprimento fixo**, e é unidirecional (não possui função **inversa**)
- Para uso em segurança, funções hash devem cumprir algumas **propriedades**



# Fundamentos de Segurança e Criptografia

## Funções Hash Criptográficas

- **Resistência à primeira inversão:** dado um resumo  $R$ , é inviável encontrar uma mensagem  $M$  tal que  $R = H(M)$
- **Resistência à segunda inversão:** dado um resumo  $R$  e uma mensagem  $M_1$  tal que  $R = H(M_1)$ , é inviável encontrar uma outra mensagem  $M_2 \neq M_1$  tal que  $R = H(M_2)$
- **Resistência a colisões:** É inviável encontrar duas mensagens  $M_1$  e  $M_2$  tais que  $H(M_1) = H(M_2)$



# Fundamentos de Segurança e Criptografia

## Criptografia Simétrica

- Chave **compartilhada** para suportar confidencialidade de dados em trânsito
- Funções de **criptação** e **descriptação** usam mesma chave  $K$  para atuar na mensagem às claras ( $m$ ) e no texto cifrado ( $c$ )
- **Propriedades**: confusão (relação entre  $K$  e  $c$  deve ser não-linear) e difusão (influência de bit de  $m$  em diversos bits de  $c$ )
- **Desafio**: como compartilhar  $K$ ?

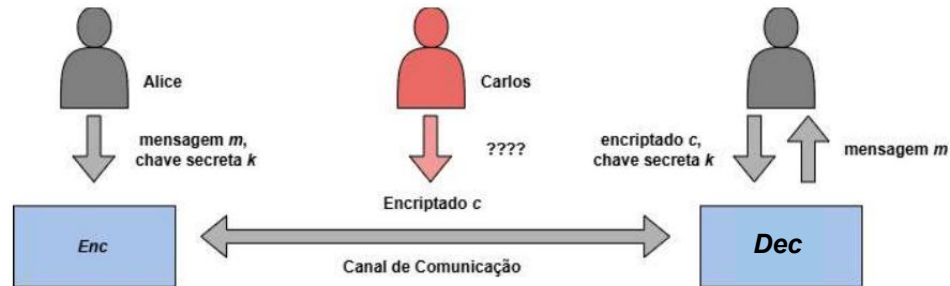


Figura 3.4. Modelo Simétrico de Criptografia. Adaptado de [Terada 2008]

# Fundamentos de Segurança e Criptografia

## Criptografia Assimétrica

- Par de Chaves: **pública** e **privada**
- Para **confidencialidade**: uso de chave pública  $pk$  para encriptar e chave privada  $sk$  para descriptar
- Para **irretratabilidade**: assinatura digital pelo remetente usando  $sk$ , verificação usando  $pk$  por terceiros
- Também utilizada para **troca de chaves** utilizadas na criptografia simétrica (*Key Encapsulation Mechanism*)

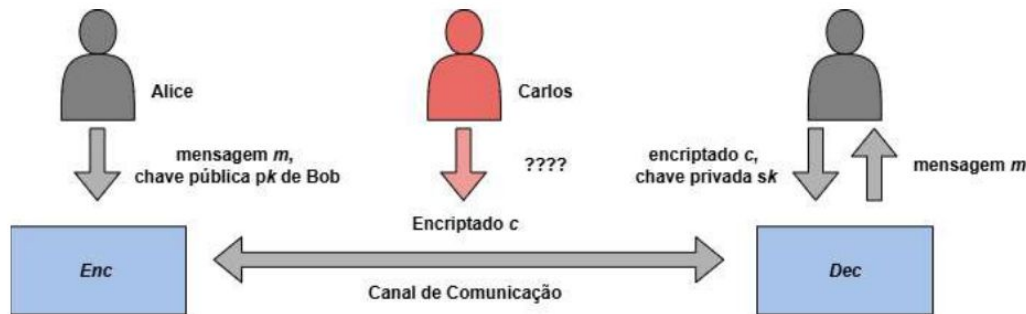


Figura 3.5. Modelo Assimétrico de Criptografia. Adaptado de [Terada 2008]

# Fundamentos de Segurança e Criptografia

## Criptografia Assimétrica

- **Assimetria de Complexidade:** Uso de funções que são fáceis de calcular em uma direção (criptação), mas difíceis de inverter (descriptação) sem o conhecimento de um informação específica  $sk$  (chave privada)
  - **Problemas matemáticos** computacionalmente difíceis, mas com solução eficiente quando informação  $sk$  está disponível (e.g., fatoração de inteiros)
  - **Fatoração de Inteiros:** dado  $N = pq$  grande, objetivo é encontrar  $p$  e  $q$ . Trivial se souber um fator (base para RSA)
  - **Desafio:** o que fazer se problema matemático se tornar tratável com a computação quântica?
1. Dois primos grandes  $p$  e  $q$  são escolhidos.
  2. O módulo  $N$  comum das operações é calculado por  $N = pq$ .
  3. A função totiente de Euler é calculada por  $\phi(N) = (p-1)(q-1)$ .
  4. O expoente público  $e$  é escolhido sendo um inteiro tal que  $1 < e < \phi(N)$  e  $\gcd(e, \phi(N)) = 1$ .
  5. O expoente privado  $d$  é calculado tal que  $d \equiv e^{-1} \pmod{\phi(N)}$ , isto é, o inverso multiplicativo de  $e$  módulo  $\phi(N)$ .

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- **Introdução à Computação Quântica**

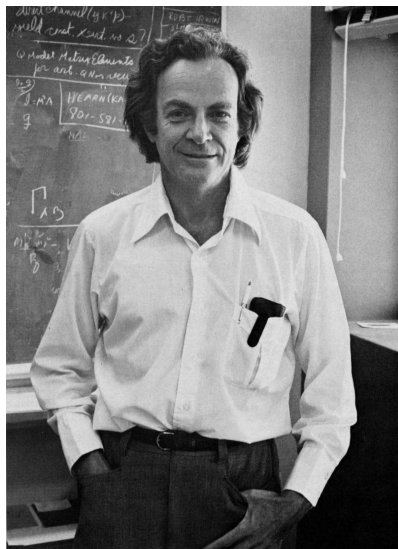
## Pausa (30 min)

## Parte 2 (1h30)

- Complexidade de Algoritmos
- Algoritmos Quânticos e seus Impactos
- Criptografia Pós-Quântica
- Oportunidades em Computação Quântica

# Introdução à Computação Quântica

*I'm not happy with all the analyses that go with just the classical theory, because **nature isn't classical**, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical ...*



Richard P. Feynman  
Department of Physics,  
California Institute of  
Technology

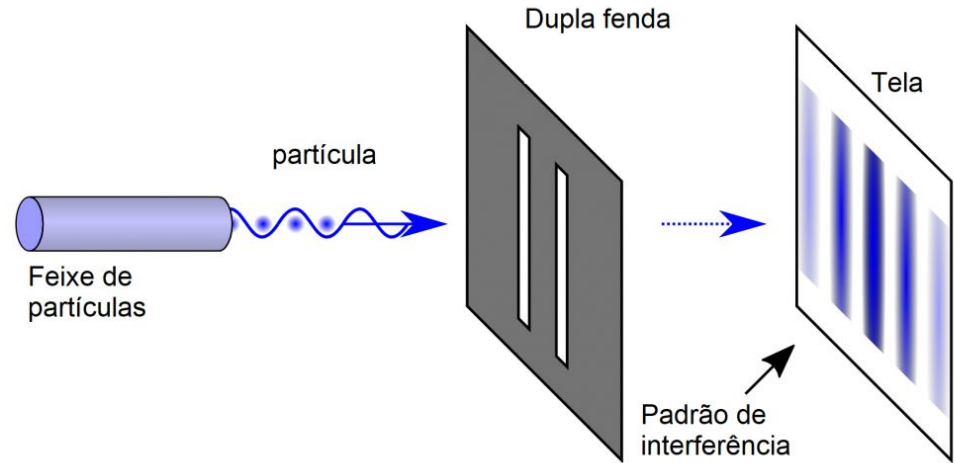
International Journal of  
Theoretical Physics,  
Vol 21, Nos. 6/7, 1982



# Introdução à Computação Quântica

## Mecânica Quântica

- Computação quântica se baseia nos fenômenos da Mecânica Quântica
- Há fenômenos que a **Mecânica Clássica** não consegue explicar
- Nível **microscópico**: leis que regem este novo paradigma de computação são diferentes do mundo macroscópico onde vivemos!



# Introdução à Computação Quântica

Visualização

Lógica (representação)

Hardware

Níveis de abstração

# Introdução à Computação Quântica

Clássico

Quântico

Visualização	119 'W'	$ 119\rangle$
Lógica (representação)	01110111	$ 01110111\rangle$
Hardware	Transistores	Sis. Quânticos

Níveis de abstração

# Introdução à Computação Quântica

No regimento clássico, não há distinção entre estado e observação (**medição**)...

0	1	1	1	0	1	1	1
---	---	---	---	---	---	---	---

=

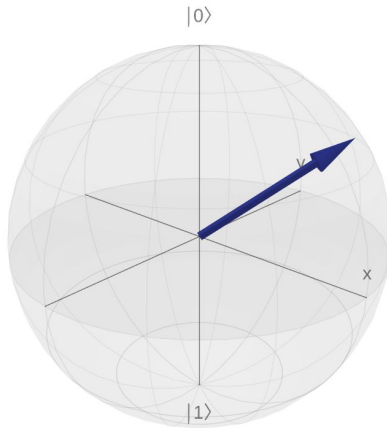
**01110111**

No computador

Resultado observado

# Introdução à Computação Quântica

... No quântico há



No computador

$\neq$

$|01110111\rangle$

Resultado observado

# Introdução à Computação Quântica

Clássico

Quântico

Visualização	Determinística	Probabilística
Lógica (representação)	Bits	Qubits
Hardware	Transistores	Sis. Quânticos

Diferenças

# Introdução à Computação Quântica

Um **qubit** é a unidade básica de informação na computação quântica. Qubits podem ser implementados fisicamente por diversos sistemas quânticos, como fótons, elétrons, íons entre outros. Um qubit, logicamente, é representado com um **vetor de estado**.

# Introdução à Computação Quântica

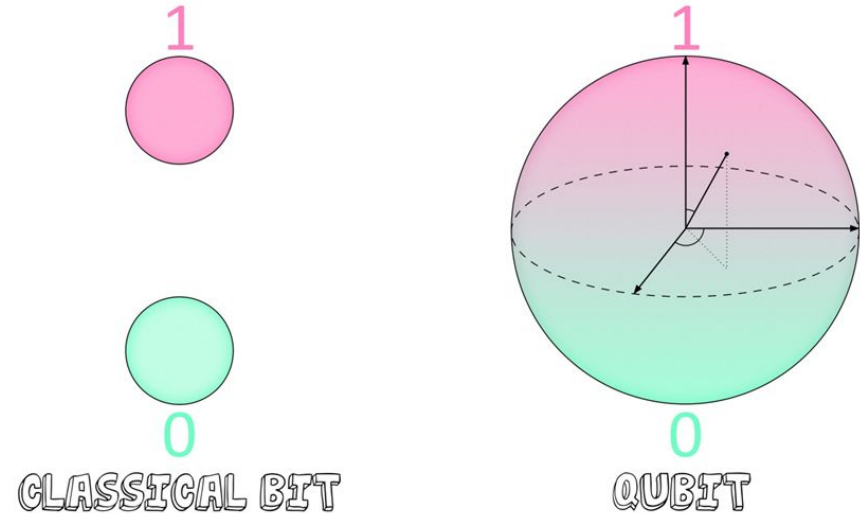
Ser implementado por um sistema quântico (e não clássico), permite que os qubits sofram a influência de fenômenos quânticos. É de especial interesse para a computação quântica 3 deles: **Superposição, Interferência e Emaranhamento.**



# Introdução à Computação Quântica

## Fenômenos Quânticos

- **Superposição** permite que um qubit represente simultaneamente 0 e 1, ao contrário dos bits clássicos que representam apenas um valor
- **Emaranhamento (Entrelaçamento)** cria uma relação entre qubits, onde a medida de um qubit instantaneamente afeta o estado dos outros qubits emaranhados (propriedade global)
- **Interferência** permite que amplitudes de probabilidade dos qubits sejam manipuladas



# Introdução à Computação Quântica

## Fenômenos Quânticos

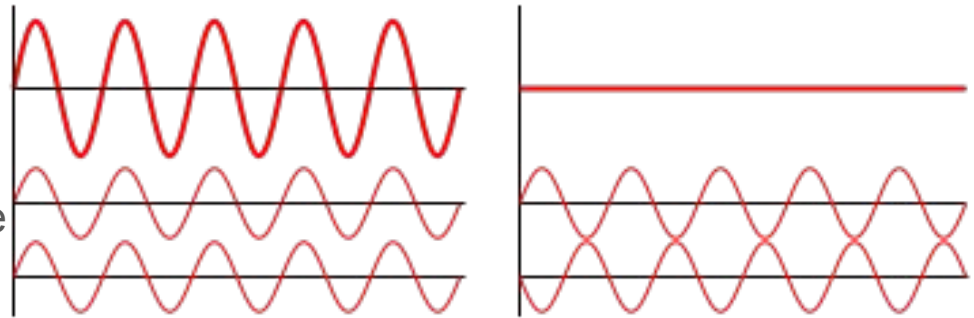
- **Superposição** permite que um qubit represente simultaneamente 0 e 1, ao contrário dos bits clássicos que representam apenas um valor
- **Emaranhamento (Entrelaçamento)** cria uma relação entre qubits, onde a medida de um qubit instantaneamente afeta o estado dos outros qubits emaranhados (propriedade global)
- **Interferência** permite que amplitudes de probabilidade dos qubits sejam manipuladas



# Introdução à Computação Quântica

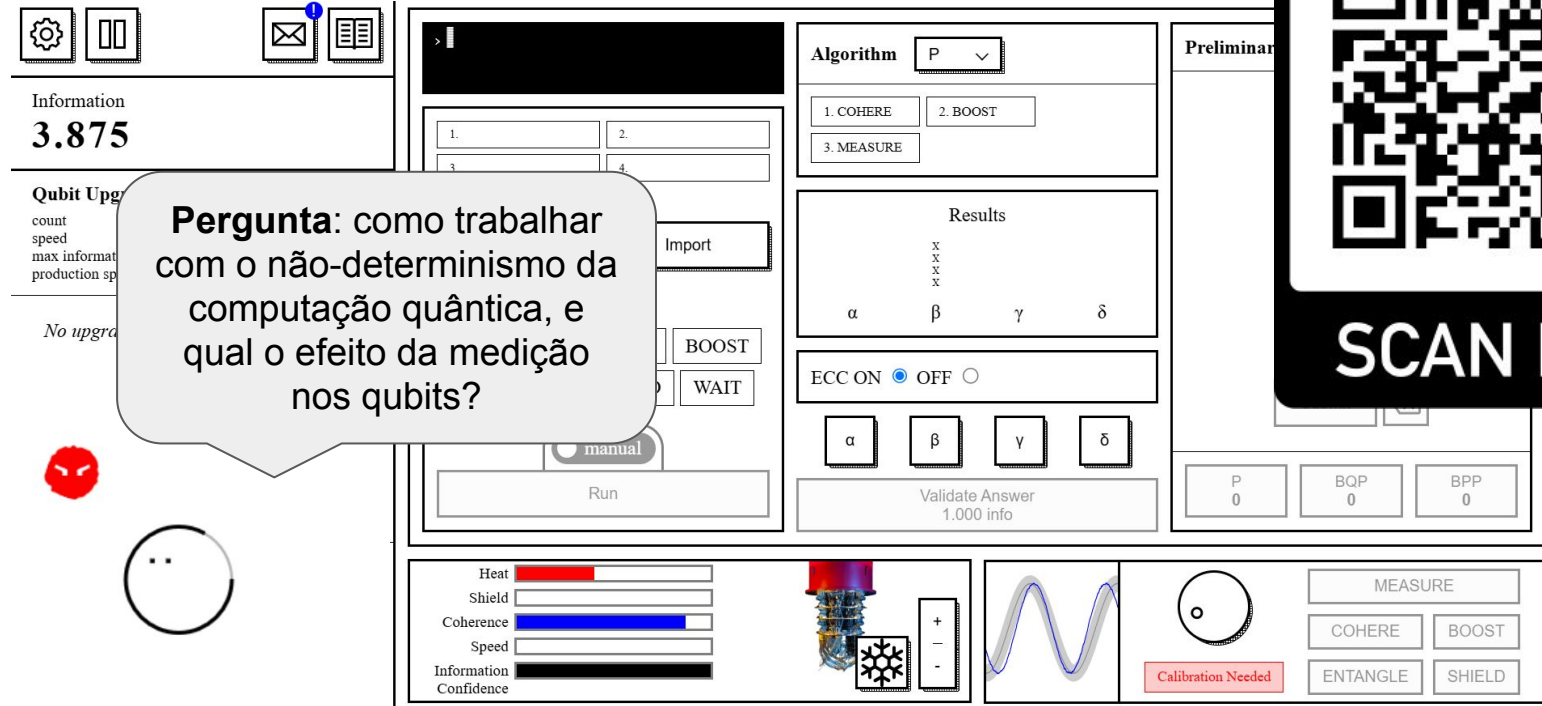
## Fenômenos Quânticos

- **Superposição** permite que um qubit represente simultaneamente 0 e 1, ao contrário dos bits clássicos que representam apenas um valor
- **Emaranhamento (Entrelaçamento)** cria uma relação entre qubits, onde a medida de um qubit instantaneamente afeta o estado dos outros qubits emaranhados (propriedade global)
- **Interferência** permite que amplitudes de probabilidade dos qubits sejam manipuladas



# Introdução à Computação Quântica

The Qubit Game (<https://quantumai.google/education/thequbitgame>)



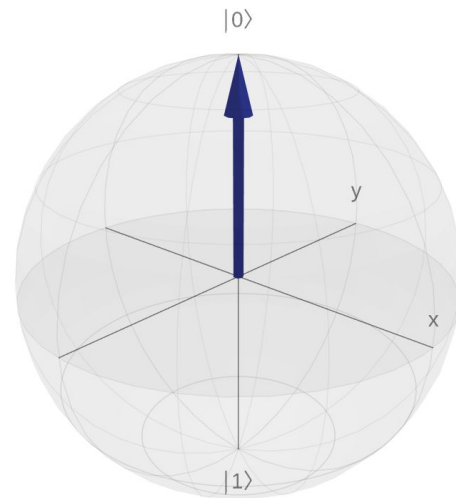
# Introdução à Computação Quântica

Notação de Dirac e vetores de estado:

$$\langle 0| = (1 \quad 0) \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Bra

Ket



[bloch.kherb.io](https://bloch.kherb.io)

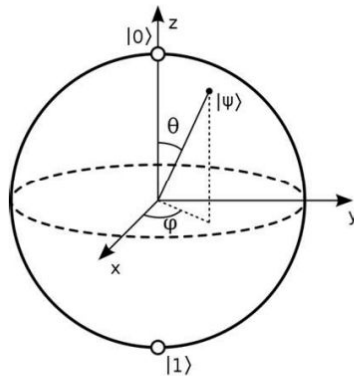
Esfera de Bloch

# Introdução à Computação Quântica

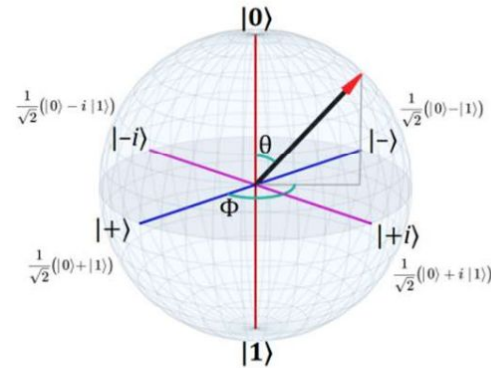
Um qubit é a unidade básica de informação na computação quântica.

A representação na **esfera de Bloch** permite modelar a **superposição**.

$$e^{i\phi} = \cos(\phi) + i\sin(\phi) \quad (11)$$



(a) Esfera de Bloch.  
Fonte: [Smite-Meister 2023]



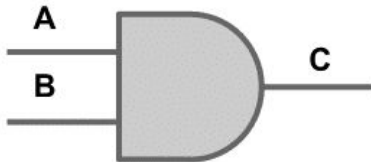
(b) Estados notáveis na Esfera de Bloch.  
Fonte: [Smythe 2021]

**Figura 3.7. Representação de estados na Esfera de Bloch**

# Introdução à Computação Quântica

Modelagem dos fenômenos de interferência para modificar as amplitudes de probabilidade associados aos estados dos qubits pode ser realizada usando a abstração de **circuitos quânticos**.

PORTA E (AND)



$$C = A \cdot B$$

A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

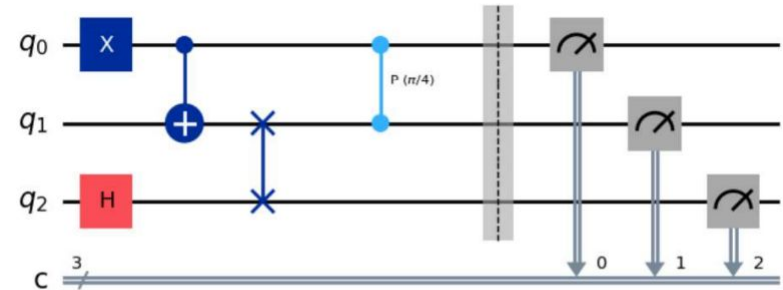


Figura 3.8. Exemplo de Circuito Quântico

# Introdução à Computação Quântica

Cada **porta quântica** pode operar em um ou mais qubits, sendo possível observar as mudanças em um único qubit usando a esfera de Bloch.

Lembrar que a **medição** também afeta os qubits, e que é necessário fazer a execução e medição do circuito diversas vezes devido ao não-determinismo.

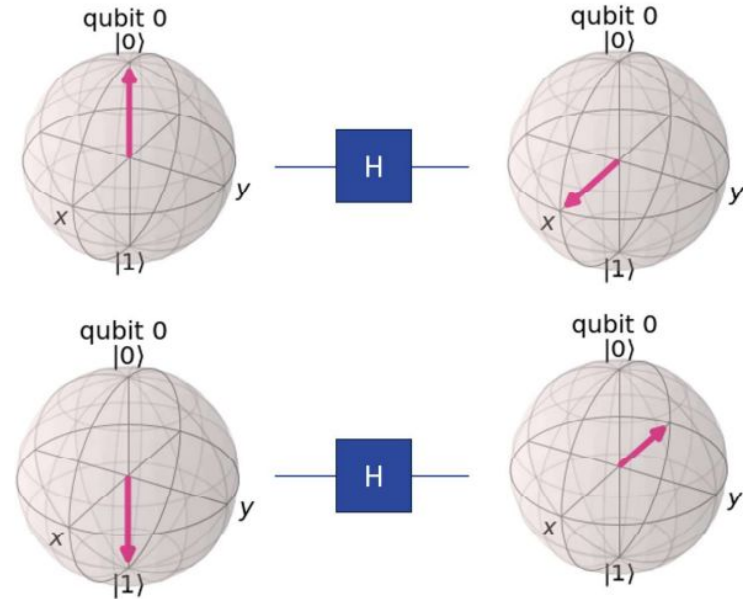
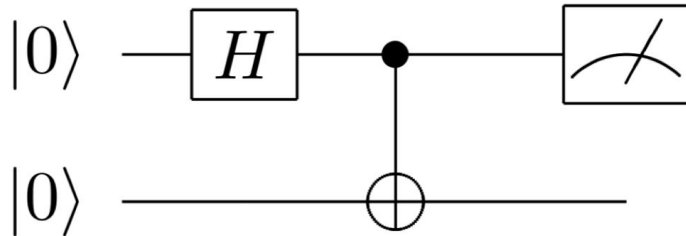


Figura 3.9. Porta H e seu efeito visualizado na esfera de Bloch



# Introdução à Computação Quântica

Exemplos de outras portas quânticas são apresentadas abaixo.

Cada **porta quântica** está associada a uma **matriz** que representa sua operação nas amplitudes de probabilidade dos qubits.

Uma propriedade importante é que essas matrizes possuem **inversa**.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (21)$$

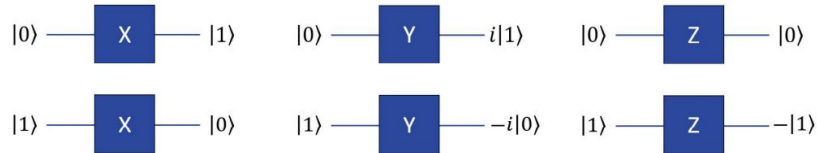


Figura 3.10. Portas de Pauli e seus efeitos sobre a base computacional

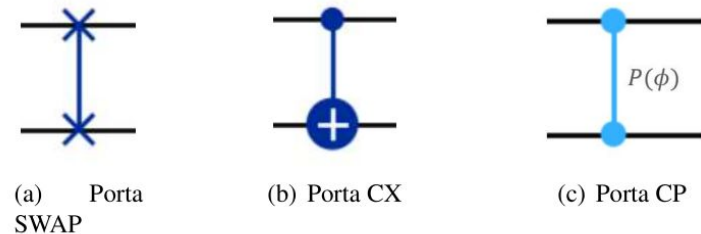


Figura 3.11. Representação gráfica das portas SWAP, CX e CP

# Introdução à Computação Quântica

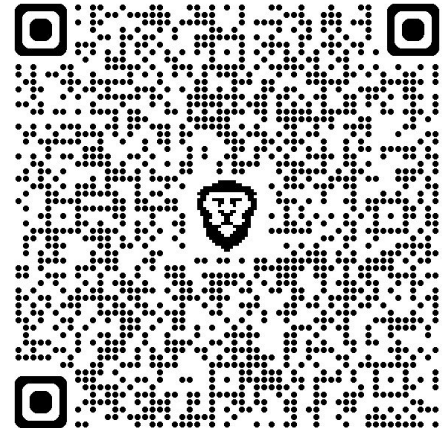
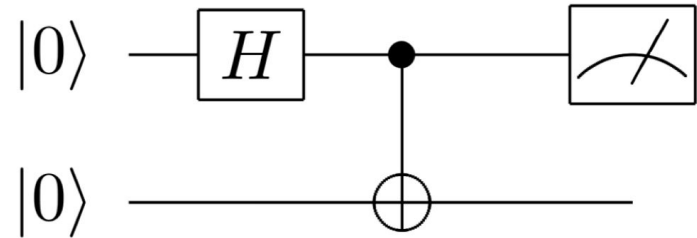
Acesse <https://quantum.cloud.ibm.com/composer> e crie sua conta.

Vamos simular o circuito quântico apresentado ao lado usando o **Composer**.

Qual o resultado esperado?

Ao aplicar portas **Hadamard** em diversos qubits, o que obtemos?

O **CNOT** modela qual dos fenômenos quânticos: **interferência**, **emaranhamento** ou **superposição**?



# Introdução à Computação Quântica

IBM Quantum Platform

Untitled circuit | File | Edit | View | Help

Operations

Left alignment | Inspect

q[0] q[1] c4

Probabilities

Computational basis states

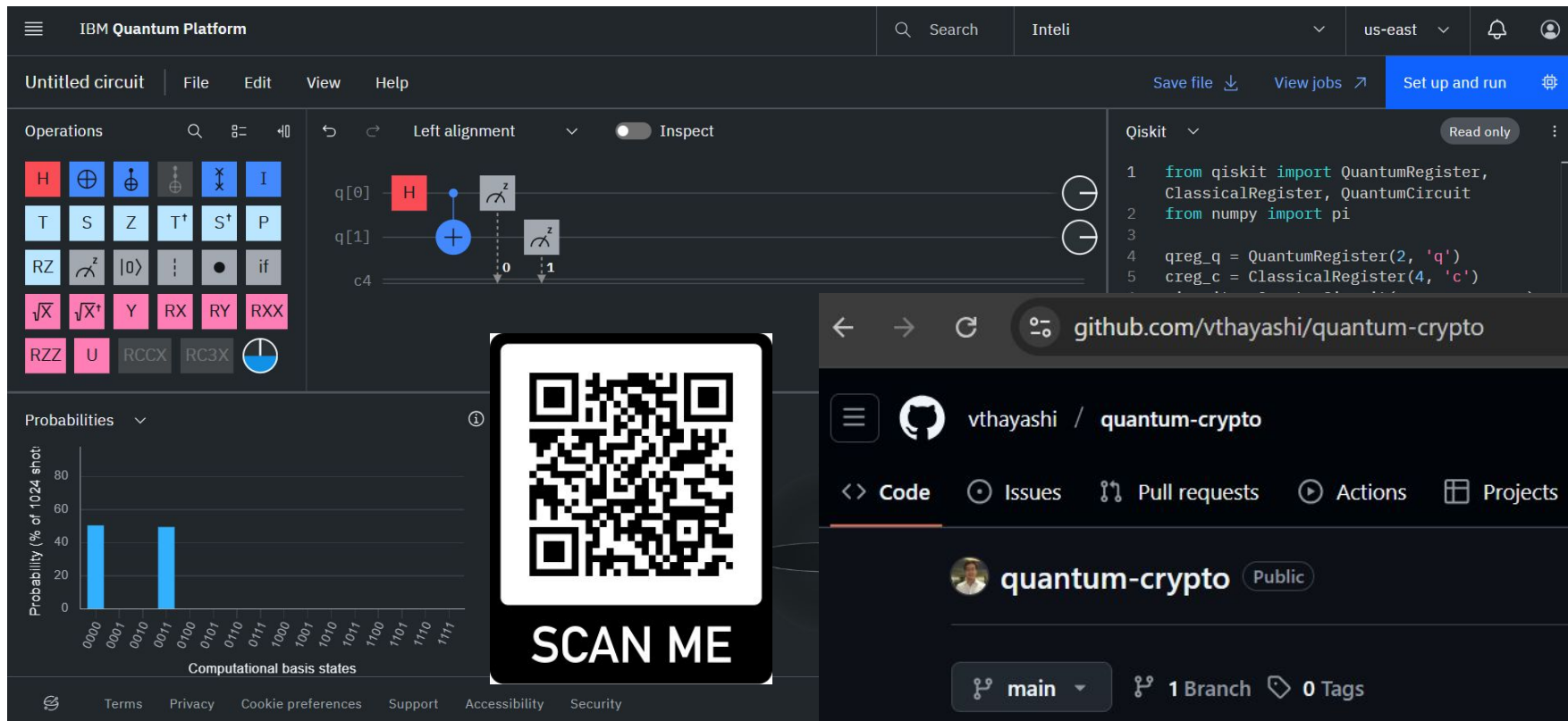
SCAN ME

github.com/vthayashi/quantum-crypto

Code | Issues | Pull requests | Actions | Projects

quantum-crypto | Public

main | 1 Branch | 0 Tags



The screenshot displays the IBM Quantum Platform interface. At the top, there's a navigation bar with 'Untitled circuit', 'File', 'Edit', 'View', and 'Help' menus. Below this, a toolbar contains 'Save file', 'View jobs', and 'Set up and run' buttons. The main workspace is divided into three sections: 'Operations' on the left with a grid of quantum gates (H, T, S, Z, T†, S†, P, RZ, RY, RX, RY, RXX, RZZ, U, RCCX, RC3X), a central circuit editor showing a circuit with qubits q[0], q[1], and a classical register c4, and a 'Probabilities' section on the bottom left showing a bar chart for computational basis states. A large QR code with the text 'SCAN ME' is overlaid on the circuit editor. On the right, a 'Qiskit' code editor shows a Python script for creating a quantum circuit. Below the circuit editor, a browser window displays the GitHub repository page for 'vthayashi/quantum-crypto'.

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- Introdução à Computação Quântica

## **Pausa (30 min)**

## Parte 2 (1h30)

- Complexidade de Algoritmos
- Algoritmos Quânticos e seus Impactos
- Criptografia Pós-Quântica
- Oportunidades em Computação Quântica

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- Introdução à Computação Quântica

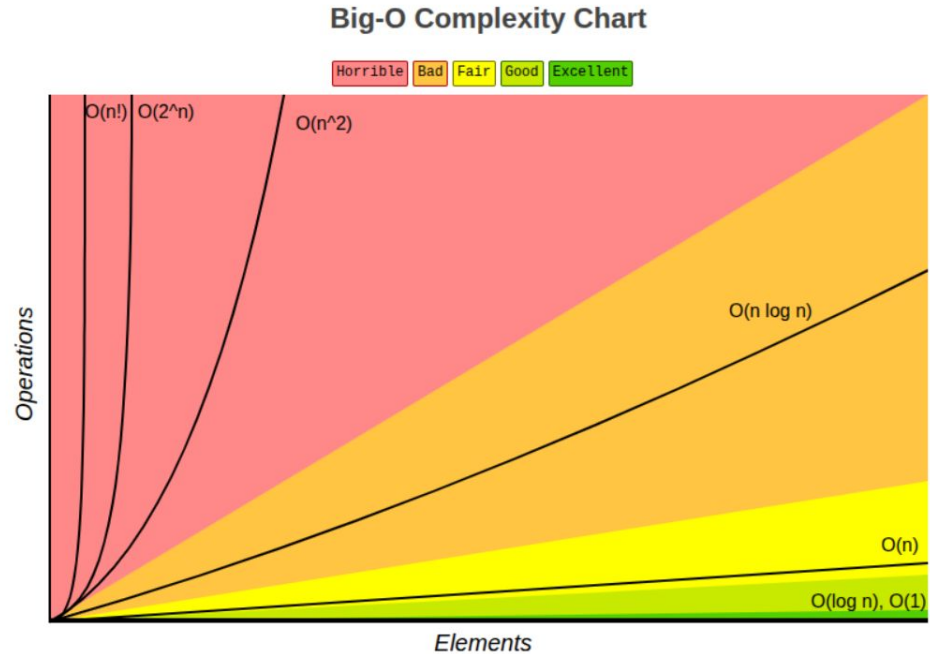
## Pausa (30 min)

## Parte 2 (1h30)

- **Complexidade de Algoritmos**
- Algoritmos Quânticos e seus Impactos
- Criptografia Pós-Quântica
- Oportunidades em Computação Quântica

# Complexidade de Algoritmos

- Ordem de grandeza do **crescimento na quantidade de passos que um algoritmo** leva para resolver um problema dado o tamanho da entrada
- **A complexidade é do algoritmo, não do problema**
- Análise **não depende** de detalhes de **implementação**, é inerente ao algoritmo
- Ou seja: levar em consideração o problema sendo tratado e quais algoritmos considerados ao comparar computação clássica com a quântica



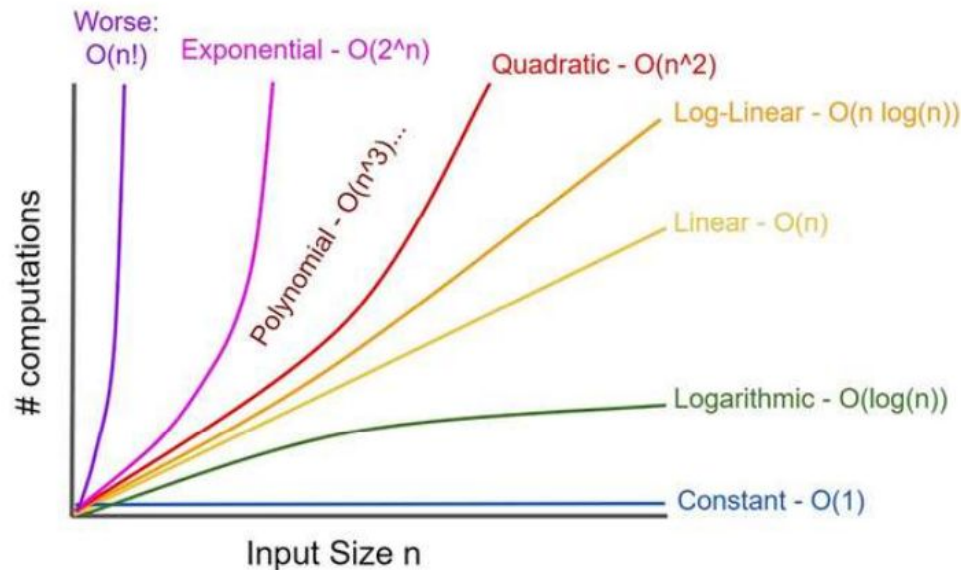
ROWELL, E. Big-O Algorithm Complexity Cheat Sheet (Know Thy Complexities!).

Disponível em: <<https://www.bigocheatsheet.com/>>.

# Complexidade de Algoritmos

## Análise Assintótica

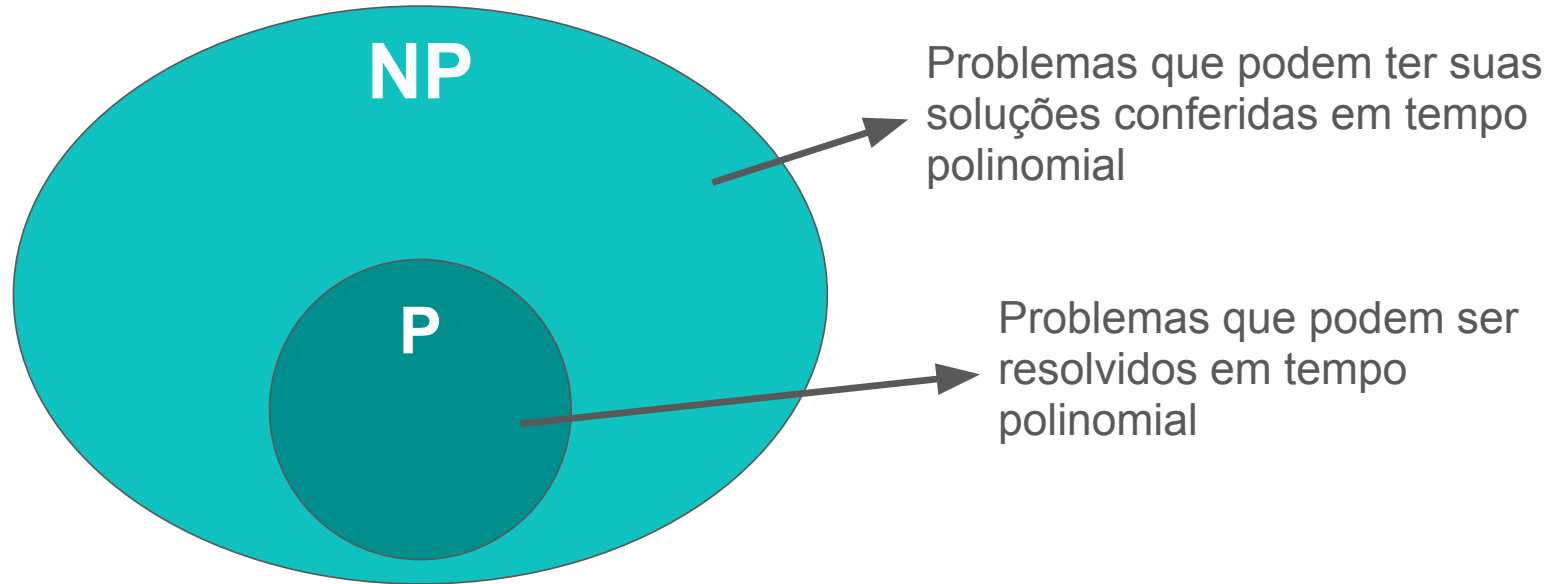
- **Big-O**: Indica o limite superior da complexidade (pior caso)
- **Big-Ω**: Indica o limite inferior da complexidade (melhor caso)
- **Big-Θ**: Indica um limite “ajustado” da complexidade (caso médio)



(b) Exemplos de funções em notação Big-O. Fonte: [Salvi 2023]

# Complexidade de Algoritmos

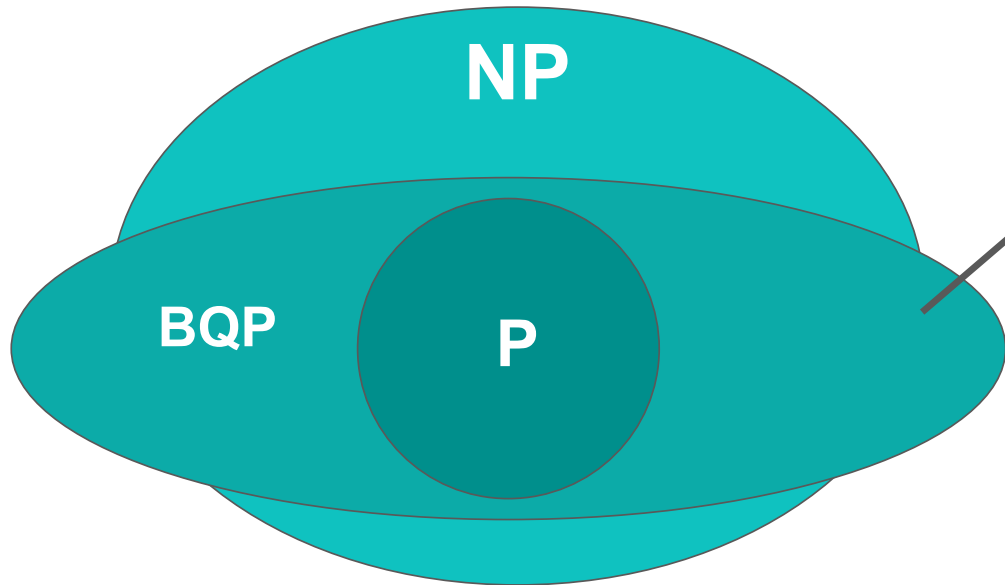
Os problemas computacionais conhecidos são classificados conforme suas características:





# Complexidade de Algoritmos

Os problemas computacionais conhecidos são classificados conforme suas características:



Problemas que podem ser resolvidos com computadores quânticos em tempo polinomial\*

\* considera-se um cenário com uma taxa de erro aceitável de até 1/3

# Complexidade de Algoritmos

## Problemas Computacionais

- Existem alguns problemas que não são tratáveis em **computação clássica**, mas são tratáveis em **computação quântica**...
- O que ocorre se algum destes problemas for **premissa** importante de um mecanismo criptográfico?
- **Importante:** ainda há problemas que não conseguimos resolver de forma eficiente, seja com computador clássico ou quântico



(a) Classificação simplificada dos problemas computacionais.

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- Introdução à Computação Quântica

## Pausa (30 min)

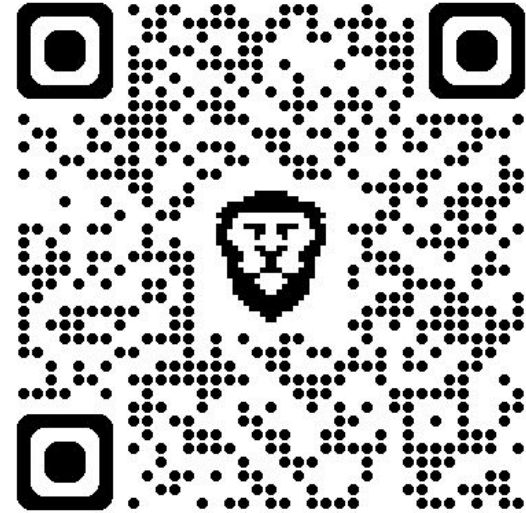
## Parte 2 (1h30)

- Complexidade de Algoritmos
- **Algoritmos Quânticos e seus Impactos**
- Criptografia Pós-Quântica
- Oportunidades em Computação Quântica

# Algoritmos Quânticos e seus Impactos

Assim como na computação clássica, existem inúmeros algoritmos quânticos com os mais variados usos.

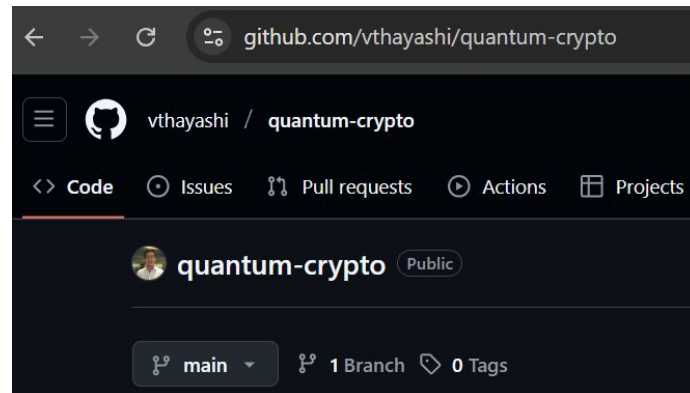
QAOA Grover Simon  
Shor HHL Deutsch QFT  
Teleportation VQE Superdense  
Coding



# Algoritmos Quânticos e seus Impactos

Assim como na computação clássica, existem inúmeros algoritmos quânticos com os mais variados usos.

QAOA  
Shor  
Grover  
HHL  
Teleportation  
VQE  
Deutsch  
Simon  
QFT  
Superdense  
Coding



# Algoritmos Quânticos e seus Impactos

## Algoritmo de Grover

- Usado para **buscas** em conjuntos de dados não-estruturados

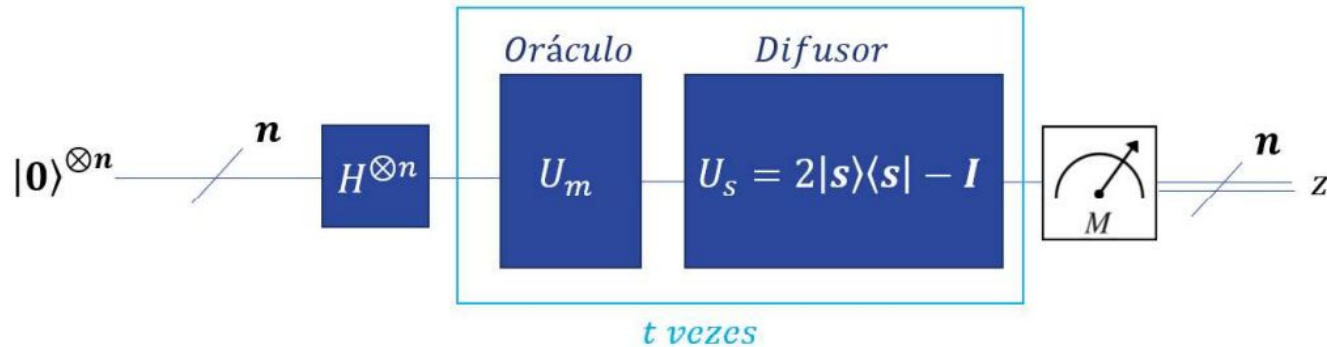
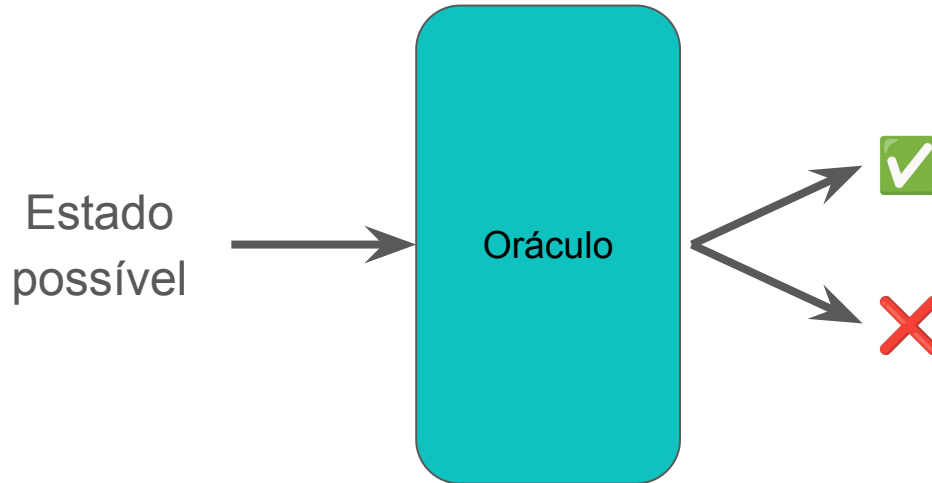


Figura 3.12. Circuito geral para executar o Algoritmo de Grover

# Algoritmos Quânticos e seus Impactos

## Algoritmo de Grover

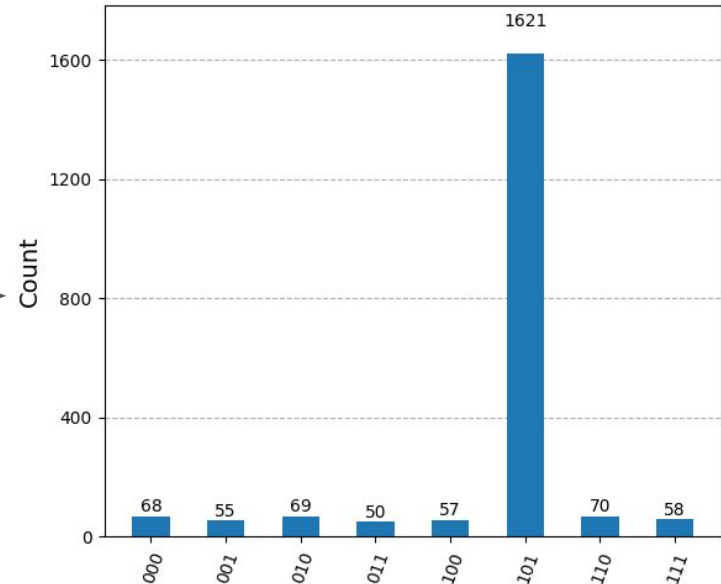
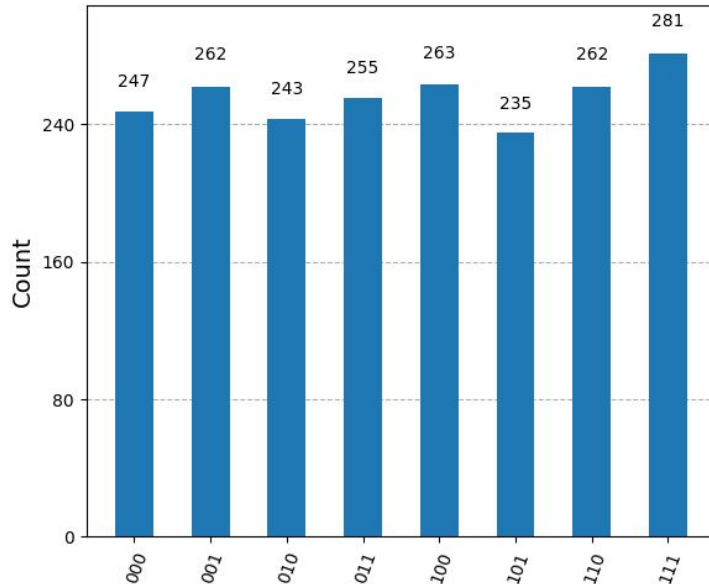
- A ideia gira em torno de uma consulta à um oráculo (dado ou construído) que é capaz de “marcar” o estado referente ao elemento de interesse, mudando sua **fase**



# Algoritmos Quânticos e seus Impactos

## Algoritmo de Grover

Após isso, o **difusor** irá amplificar a amplitude do estado de interesse, permitindo diferenciá-lo dos outros estados:

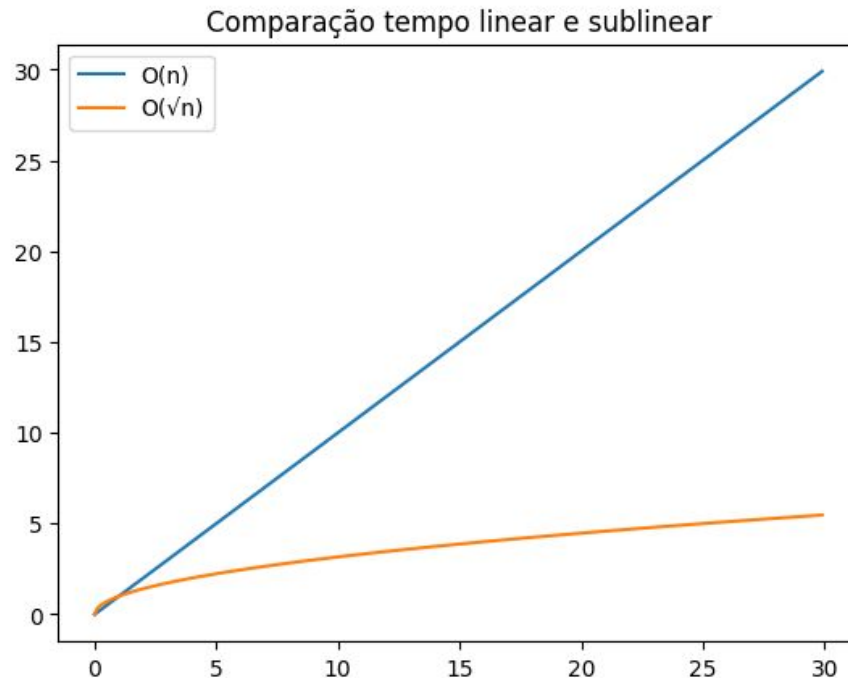




# Algoritmos Quânticos e seus Impactos

## Algoritmo de Grover

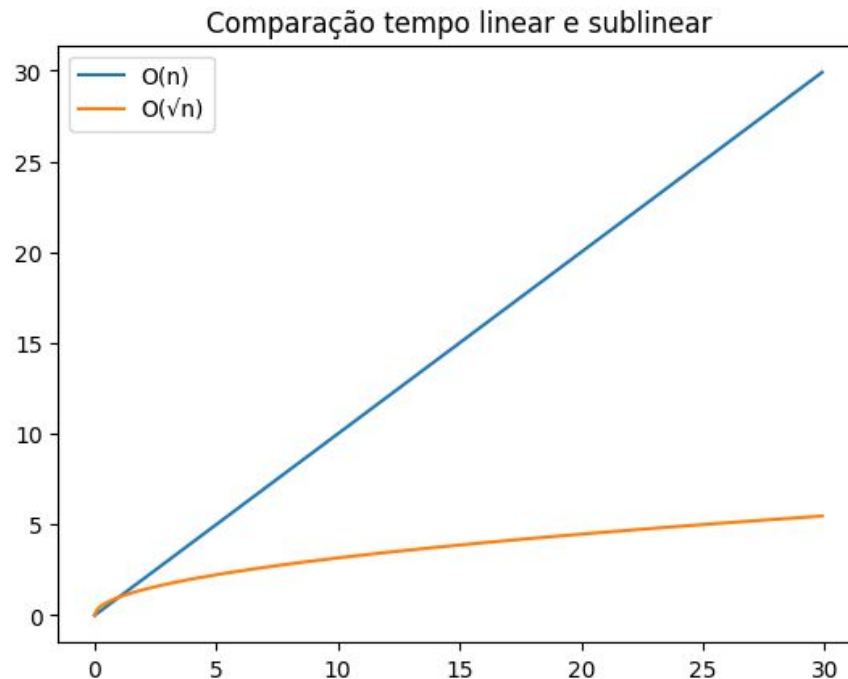
- O Algoritmo de Grover reduz a complexidade de tempo da busca de **linear** para **sublinear**:  $O(n) \rightarrow O(\sqrt{n})$
- Tendo uma quantidade grande o suficiente de pares mensagem/encryptado, é possível criar a porta oráculo e usar o Algoritmo de Grover para achar a **chave simétrica** indicada
- Também é possível utilizar Grover no cenário de uso de **funções hash**



# Algoritmos Quânticos e seus Impactos

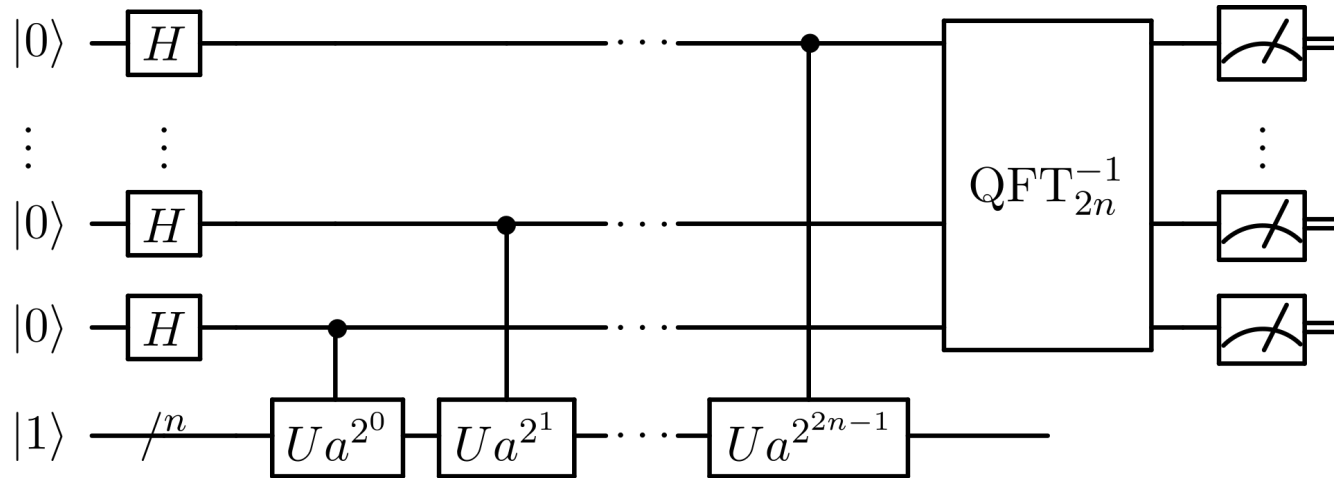
## Algoritmo de Grover

- Em sistemas de criptografia **simétrica**, como AES, a segurança está diretamente relacionada ao tamanho da chave
- Apesar do **aceleração quadrática** do Algoritmo de Grover, ela não é crítica para esses sistemas
- O **aumento do tamanho das chaves** se apresenta como uma contramedida eficiente
- Raciocínio similar para impactos de Grover em **funções hash** criptográficas



# Algoritmos Quânticos e seus Impactos

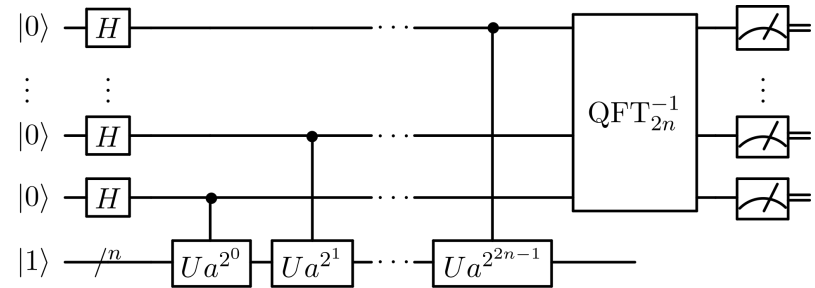
## Algoritmo de Shor



# Algoritmos Quânticos e seus Impactos

## Algoritmo de Shor

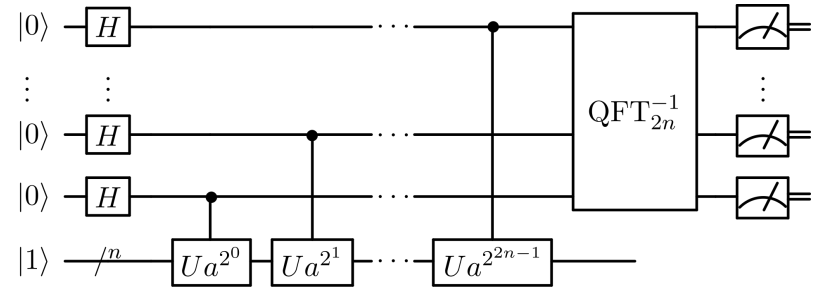
- Pode ser usado para **fatorar números inteiros** (dado  $N = pq$  sendo  $p$  e  $q$  números primos, achar  $p$  e  $q$ )
- Pode ser usado para calcular logaritmos discretos (dados número primo  $p$  e inteiros  $g$  e  $y$ , encontrar  $x$  que satisfaz  $y = g^x \text{ mod } p$ )
- Ambas aplicações podem ser realizadas de forma eficiente, com **aceleração exponencial** quando comparado aos melhores algoritmos clássicos (e o problema é que são as bases da criptografia de chave pública usada hoje...



# Algoritmos Quânticos e seus Impactos

## Algoritmo de Shor

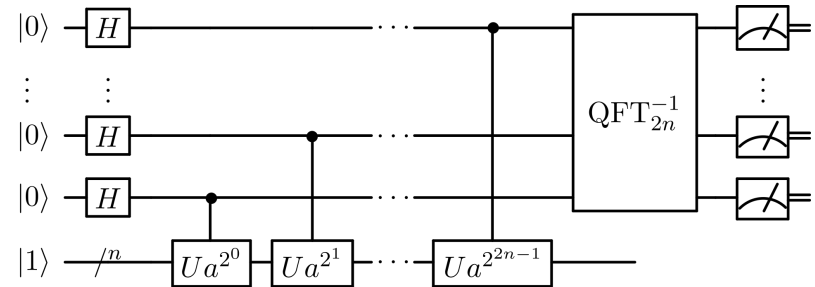
- **Ideia principal:** transformar problema da fatoração ou de cálculo de logaritmo discreto no problema de **encontrar o período de uma função** em **tempo polinomial** usando um computador quântico
- Peter Shor provou ser possível fazer esta transformação, portanto resolver estes problemas usando um algoritmo de complexidade **polinomial** frente aos clássicos que possuem complexidade do **domínio exponencial**



# Algoritmos Quânticos e seus Impactos

## Algoritmo de Shor

- Portanto, mecanismos assimétricos como **RSA** e **ECC** ficam vulneráveis e podem ser quebrados quando existir um **computador quântico com escala suficiente** para executar o algoritmo de Shor para quebrar as chaves com os tamanhos utilizados hoje
- Dada a relevância do **impacto**, há a necessidade de **transição criptográfica** para evitar ataques como *Store Now Decrypt Later* (SNDL) ou *Harvest Now Decrypt Later* (HNDL)



# Algoritmos Quânticos e seus Impactos

**Tabela 3.1. Resumo dos Impactos em Criptografia.**

Primitiva Criptográfica	Exemplos de Algoritmos	Problema Subjacente	Complexidade Temporal Clássica	Complexidade Temporal Quântica	Contramedida
Hash	SHA-2, SHA-3	Cálculo de pré-imagem	$O(2^n)$	$O(2^{n/2})$	Ajustar o tamanho do <i>hash</i> se necessário
Simétrica	AES, ChaCha20	Busca de chave	$O(2^n)$	$O(2^{n/2})$	Ajustar o tamanho da chave se necessário
Assimétrica	RSA	IFP	$O(e^{(n)^\alpha (\log n)^{1-\alpha}})$	$O(poly(n))$	Substituir algoritmos
	DH, DSA, ElGamal ECDH, ECDSA, EdDSA	DLP ECDLP	$0 < \alpha < 1$ $O(e^{poly(n)})$		

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- Introdução à Computação Quântica

## Pausa (30 min)

## Parte 2 (1h30)

- Complexidade de Algoritmos
- Algoritmos Quânticos e seus Impactos
- **Criptografia Pós-Quântica**
- Oportunidades em Computação Quântica



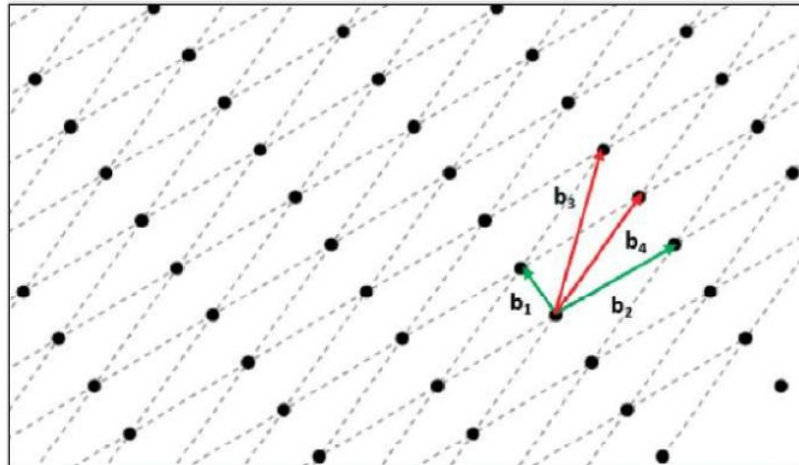
# Criptografia Pós-Quântica

- **Importante:** Criptografia Pós-Quântica (PQC - do inglês *Post-Quantum Cryptography*) é implementada em computador clássico, a premissa é que o adversário pode ter acesso a um computador quântico criptograficamente relevante (e.g., para executar o algoritmo de Shor)
- **Lembrando:** impactos menores do Algoritmo de **Grover** em **funções hash** e **criptografia simétrica** (mudança de configuração de tamanho de chaves é uma contramedida efetiva); impactos maiores do Algoritmo de **Shor** em **criptografia de chave pública**
- Diferentes classes de **problemas matemáticos** estão sendo analisados para compor o alicerce de PQC. Estes problemas devem ser computacionalmente intratáveis em computadores **clássicos** e para os quais não existam algoritmos **quânticos** eficientes

# Criptografia Pós-Quântica

**Tabela 3.2. Principais classes de problemas em criptografia pós-quântica, suas dificuldades matemáticas e exemplos de algoritmos. Adaptado de [Beullens et al. 2021]**

Classe	Fonte da Dificuldade	Exemplos de Algoritmos
Baseada em Reticulados	Problemas de reticulados euclidianos, como LWE e Module-LWE	Kyber, Dilithium, Falcon, SABER
Baseada em Códigos	Problema de Decodificação de Erros	Classic McEliece, BIKE, HQC
Baseada em Hashes	Colisões e pré-imagens em funções <i>hash</i> seguras (ex. SHA-3)	SPHINCS+
Baseada em Isogenias	Problema da Isogenia Supersingular	SIKE
Baseada em Sistemas Multivariados	Problema MQ (Multivariate Quadratic) sobre $\mathbb{F}_q$	Rainbow, GeMSS



**Figura 3.13.** Representação de um reticulado (*lattice*) no plano com duas bases distintas. Os vetores  $b_1$  e  $b_2$  (em verde) formam uma base do reticulado, enquanto os vetores  $b_3$  e  $b_4$  (em vermelho) representam uma base alternativa. Todos os pontos pretos no plano representam os pontos do reticulado gerado por combinações lineares inteiras dessas bases. Adaptado de [Shah et al. 2025].

# Criptografia Pós-Quântica

**Tabela 3.3. Resumo da evolução dos candidatos no processo de padronização NIST para criptografia pós-quântica (PQC). Em negrito, o número de algoritmos finalistas; entre parênteses, o número de algoritmos com avaliação pendente. Adaptado de [Paar et al. 2024] e [Alagic et al. 2025].**

<b>Etapa</b>	<b>Data de Anúncio</b>	<b># KEM</b>	<b># Assinatura Digital</b>
Submissões Iniciais	Dez 2017	40	29
Após 1ª Rodada	Jan 2019	17	9
Após 2ª Rodada	Jul 2020	4 + (5)	3 + (3)
Após 3ª Rodada	Set 2022	<b>4</b> + (5)	<b>3</b> + (3)

# Criptografia Pós-Quântica

- **CRYSTALS-KYBER**: padrão FIPS 203 com o nome ML-KEM (*Module Lattice-Based Key Encapsulation Mechanism*)
- **CRYSTALS-DILITHIUM**: padrão FIPS 204 com o nome ML-DSA (*Module Lattice-Based Digital Signature Algorithm*)
- **SPHINCS+**: padrão FIPS 205 com o nome SLH-DSA (*Stateless Hash-Based Digital Signature Algorithm*)
- **Falcon** foi selecionado para assinatura digital (padrão pendente)
- **HQC** (*Hamming Quasi-Cyclic*) foi selecionado para encapsulamento de chaves (padrão pendente)
- Padrões criptográficos como RSA e ECC são depreciados a partir de **2030**, e não são mais autorizados para assinatura digital e encapsulamento de chaves a partir de **2035**

# Agenda

## Parte 1 (1h30)

- Fundamentos de Segurança e Criptografia
- Introdução à Computação Quântica

## Pausa (30 min)

## Parte 2 (1h30)

- Complexidade de Algoritmos
- Algoritmos Quânticos e seus Impactos
- Criptografia Pós-Quântica
- **Oportunidades em Computação Quântica**

# Oportunidades em Computação Quântica

## Criptografia Quântica

- Uso de fenômenos quânticos para **comunicação quântica**
- **Quantum Key Distribution (QKD)** para distribuição de chaves
- Exemplo: uso de polarização de fótons (protocolo **BB84**)
- Qualquer tentativa de espionagem (medição) causa perturbação **perceptível**
- Porém possui **alto custo** associado (hardware específico)

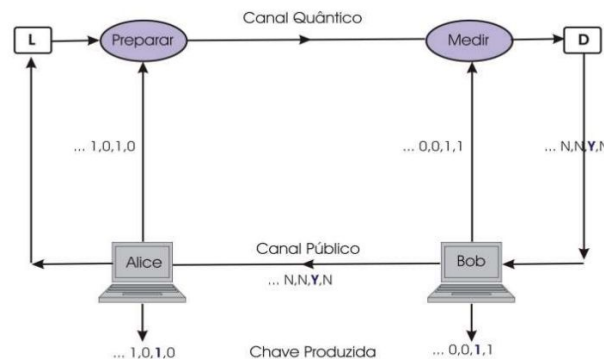


Figura 3.14. Processo completo do QKD. Adaptado de [Takagi 2003]

- Fonte: ([A typology of quantum algorithms](#), 2024)



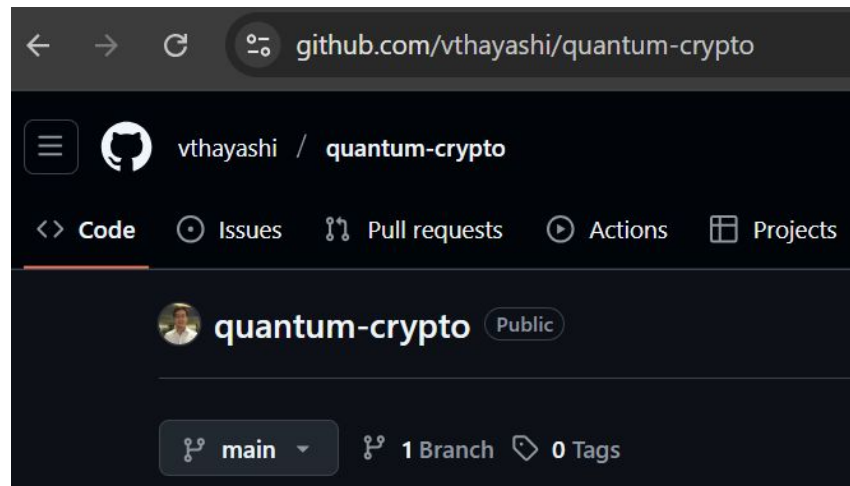


# Considerações Finais

**Objetivo:** Introduzir os fundamentos da computação quântica, examinar seus impactos na criptografia e apresentar soluções como a criptografia pós-quântica

## Capítulo de Livro do Minicurso 3

- Introdução
- Fundamentos de Criptografia
- Introdução à Computação Quântica
- Impactos em Criptografia e Soluções
- Oportunidades em Computação Quântica
- Considerações Finais
- Referências



# Considerações Finais

- **Dilemas Éticos** no uso da Tecnologia: não está acessível a todos...
- **Transição PQC**: há desafios organizacionais e outros processos relacionados em sistemas complexos
- **Iniciativas de Educação**: cursos livres no Banco Bradesco, disciplina de graduação e de pós-graduação no Inteli, disciplina de pós-graduação na Escola Politécnica da USP
- **2025 International Year of Quantum Science and Technology** (pela Organização das Nações Unidas - ONU)



Fig. 2. CSF Functions

# Considerações Finais

## CSO



Home • Security • Chinese researchers break RSA encryption with a quantum computer

by Gyana Swain

## Chinese researchers break RSA encryption with a quantum computer

News

14 Oct 2024 • 4 mins

Data and Information Security

Encryption



The research team, led by Wang Chao from Shanghai University, found that D-Wave's quantum computers can optimize problem-solving in a way that makes it possible to attack encryption methods such as RSA.

## How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

May 23, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrötenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrötenloher 2024.

# Minicurso 3 - Introdução à Computação Quântica e Impactos em Criptografia

**Victor Hayashi** (Poli-USP), Bryan Ferreira (IME-USP), **Reginaldo Arakaki** (Poli-USP), Jonatas Rossetti (Bradesco), Routo Terada (IME-USP), Ever Costa (Inteli), **Wildisley Filho** (Inteli), Giovanna Vieira (Inteli), Luiza Petenazzi (Inteli), Priscila Falcão (Inteli)

**Obrigado!**