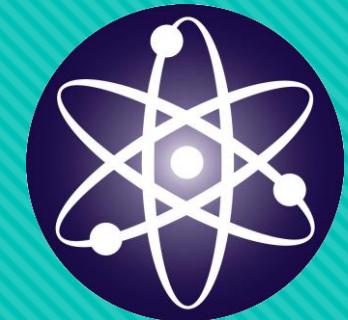


Computação Quântica



Introdução a computação quântica
Computadores Quânticos
Algoritmo de Shor

Computação clássica

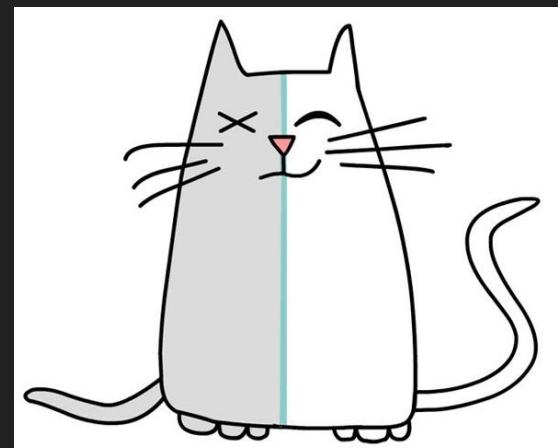
- A ciência da computação nasceu com o notável artigo do matemático inglês Alan Turing em 1936.
- Toda a informação fornecida a um computador é lida, processada e retornada sob a forma de sequências de bits.
- A tese de Church-Turing.

Computação clássica

- Em 1950 eram necessários 10^{19} átomos (10 bilhões de bilhões) para representar um único bit de informação.
- Há projeções que indicam que em poucos anos, um bit será representado por apenas um átomo.
- Lei de Moore e a limitação da mecânica clássica.

Mecânica quântica

- Levou tempo para que se notasse a conexão entre os conceitos de informação e computação e as propriedades de sistemas físicos microscópicos.
- A superposição de estados, apesar de parecer um pouco estranha, pode ser entendida mediante uma analogia conhecida como gato de Schroedinger.

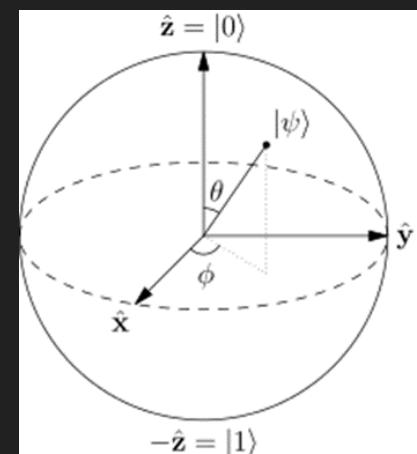


Mecânica quântica

- A única forma de averiguar o que “realmente” aconteceu com o gato será realizar uma medida: abrir a caixa e olhar dentro.
- Isso é uma forma simplista de explicar o que chamamos de colapso da função de onda.

Bits quânticos

- Um q-bit pode existir num estado contínuo entre $|0\rangle$ e $|1\rangle$ até que ele seja observado.
- Esses qubits poderiam existir simultaneamente como uma combinação de todos os números de dois bits possíveis quando se têm dois qubits.



Computação quântica

- Com a utilização da Computação Quântica a redução de tempo necessário para executar certas tarefas é enorme.
- A principal vantagem de um computador quântico é o chamado “paralelismo quântico”.

Computação quântica

- O interesse pela computação quântica teve início quando Feynman apontou, em 1982, que os sistemas clássicos não seriam capazes de modelar eficientemente os sistemas quânticos.
- Deutsch foi o primeiro a levantar o questionamento de uma real maior capacidade de processamento dos computadores quânticos em 1985.

Computação quântica

- Isto só mudou quando, em 1994, Shor publicou o seu algoritmo quântico que resolve o problema de fatoração de números inteiros grandes.
- Enquanto o número de algoritmos quânticos crescia, os esforços no sentido de produzir um hardware quântico também aumentavam.

Computação quântica

Tamanho do número a ser fatorado (em bits)	Tempo de fatoração por algoritmo clássico	Tempo de fatoração por algoritmo quântico
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de ano	36 minutos
4096	100 bilhões de quadrilhões de ano	4,8 horas

Desafios da computação quântica

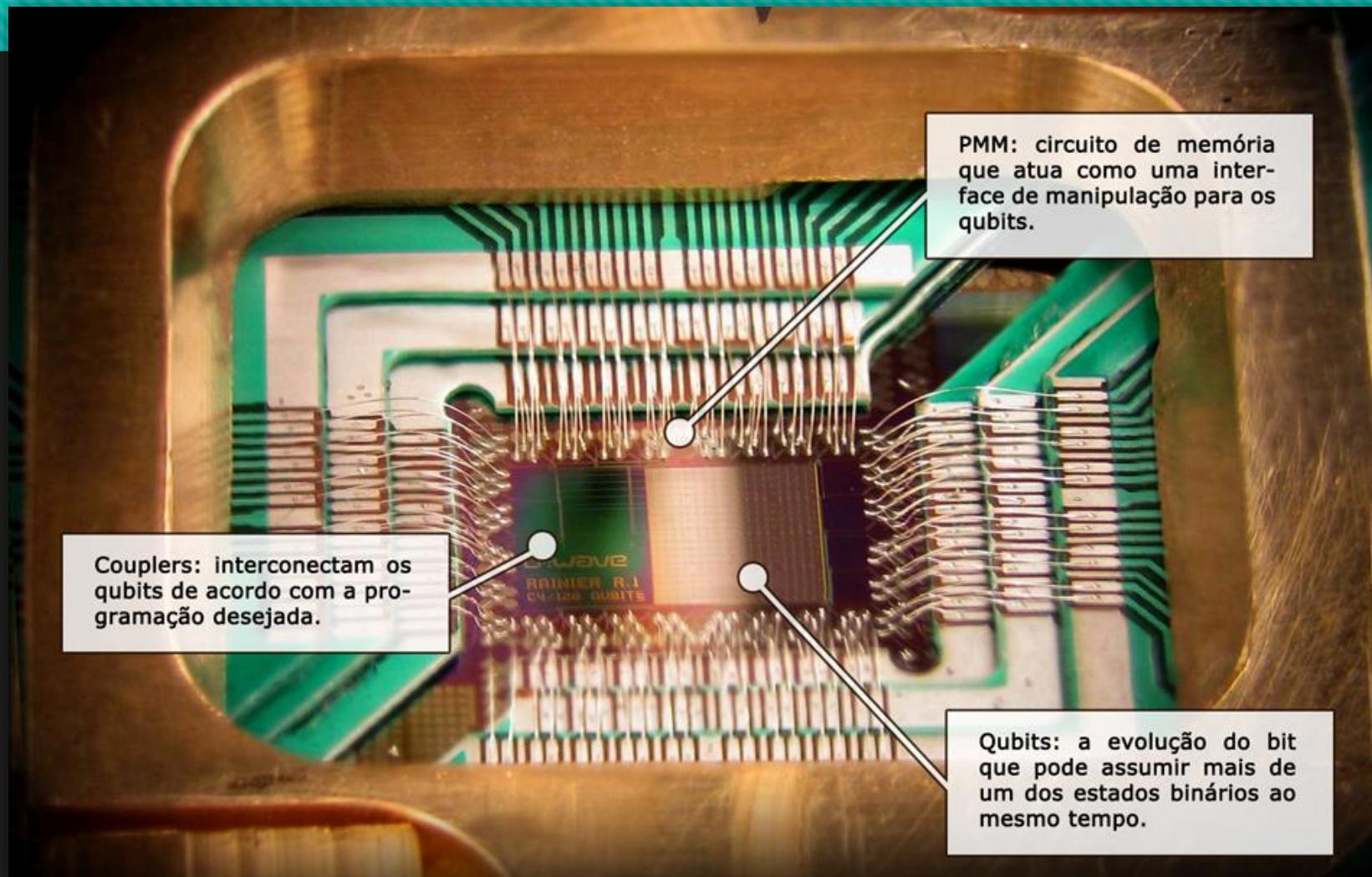
- A computação quântica experimental está enfrentando atualmente um panorama muito parecido ao que a computação clássica.
- O grande desafio atual é o aumento do número de qubits de forma controlada, e, certamente, as pesquisas pertinentes a esse tema se apoiarão na nanotecnologia.

Desafios da computação quântica



Computadores Quânticos

Um computador quântico é em princípio, um dispositivo que usa as leis da Mecânica Quântica para processar informação.



- Vantagem: O “parallelismo quântico” que é baseado numa das propriedades mais estranhas da Mecânica Quântica, a sobreposição coerente de estados distintos. Em vez de um-ou-outro, como na lógica digital, um bit quântico poderia ser ambos e, ou seja, representar 0 e 1 ao mesmo tempo.

- Requisitos necessários:

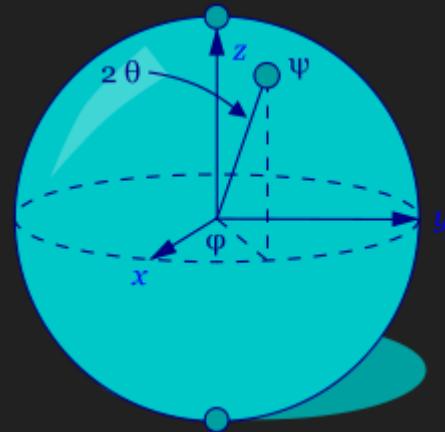
Armazenamento

Isolamento

Leitura

Portas lógicas

Precisão



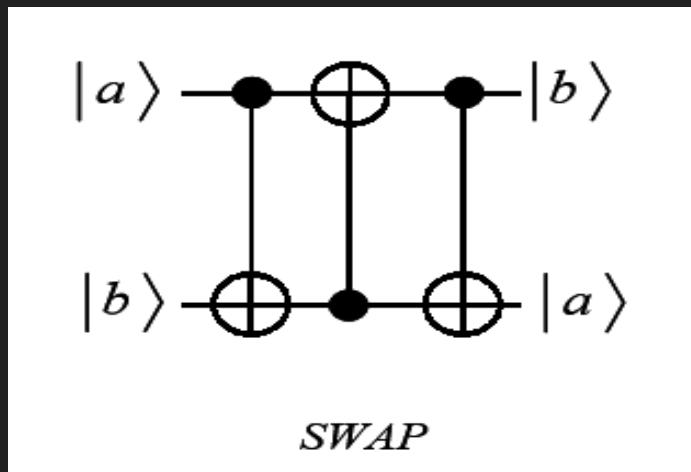
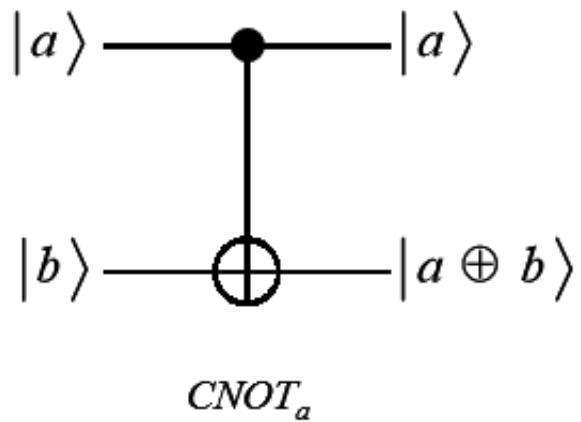
**Esfera de Bloch com
representação de um q-bit
genérico $|\psi\rangle$ e dos q-bits $|0\rangle$ e $|1\rangle$**

Exemplos de Qubits:

- O Spin nuclear
- O elétron e o spin eletrônico em nanoestruturas semicondutoras
- Dois estados atômicos
- Fóttons: estados de polarização e número
- Fluxo do campo magnético em uma junção de Josephson

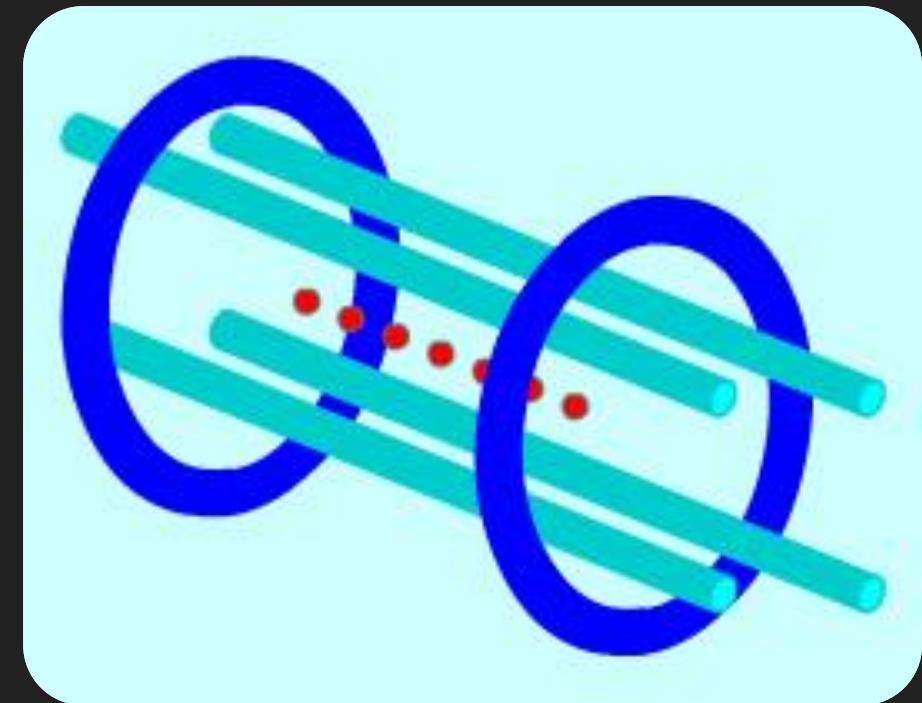
Chaves Lógicas e Circuitos Quânticos

Os circuitos quânticos são compostos de linhas e símbolos. As linhas representam os q-bits (uma linha para cada q-bit), necessários para realizar uma determinada operação e os símbolos representam as chaves lógicas.



Abordagens para implementação: Armadilha de íons

O Um íon é um átomo com excesso ou falta de elétrons. Sendo eletricamente carregados, os íons podem ser capturados usando campos elétricos e magnéticos. Feixes de laser são usados para preparar e inspecionar os íons individualmente. O elétron externo de cada íon é manipulado para ficar em duas órbitas diferentes próximas ao núcleo. Cada íon representa consequentemente um qubit. Quando um íon espalha fótons vindo do laser ele ricocheteia. Isto é sentido pelos outros íons. Este movimento é equivalente à transmissão de dados de um computador clássico.

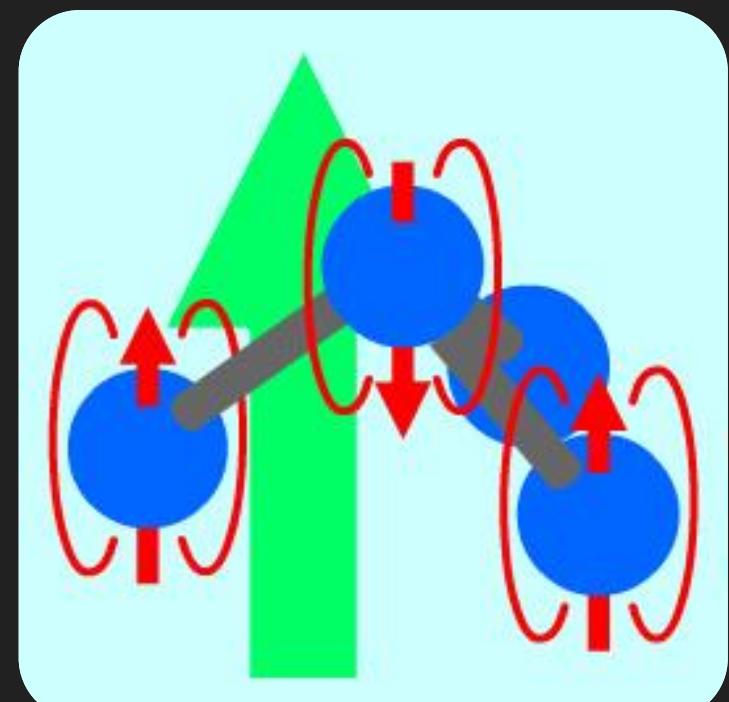


Eletrodinâmica quântica cavidade

- A ideia é aprisionar vários átomos neutros dentro de uma cavidade ótica de altíssima qualidade. A informação quântica pode, então, ser armazenada dentro dos estados internos dos átomos. Contudo, aqui os átomos interagem indiretamente através do seu acoplamento com o modo normal do campo eletromagnético na cavidade (ao invés de modos vibracionais como na armadilha de íons).

Ressonância magnética nuclear

- Devido a sua natureza quântica, o momento magnético nuclear pode estar alinhado ou no mesmo sentido do campo magnético ou no sentido oposto. Assim a orientação do núcleo se restringe apenas a esses dois valores, representando dessa forma um qubit. Dois núcleos adjacentes também afetam um ao outro através de seus momentos magnéticos, da mesma forma que dois ímãs são colocados um do lado do outro.



Implementações físicas de computadores quânticos

Computadores quânticos à base de supercondutores:

Supercondutividade é o fenômeno que ocorre quando certos materiais se encontram abaixo de uma temperatura crítica intrínseca a esse material, levando a que não tenham qualquer resistência elétrica.

Este fenômeno é usado na construção de aparelhos como a junção de Josephson (Josephson junction) e os SQUID, dispositivos supercondutores de interface quântica que por sua vez são usados na construção de computadores quânticos deste tipo.

D-Wave – Primeiro computador quântico comercial

Para tirar vantagem dos efeitos quânticos, o DW requer condições extremas e muito específicas. Ele precisa operar a 0,02 Kelvin (-273,13°C), 150 vezes mais frio do que as profundezas do espaço interestelar, em um vácuo cuja pressão atmosférica é 10 bilhões de vezes menor que a normal. Ele ainda precisa de blindagem pesada para se proteger contra interferência magnética.

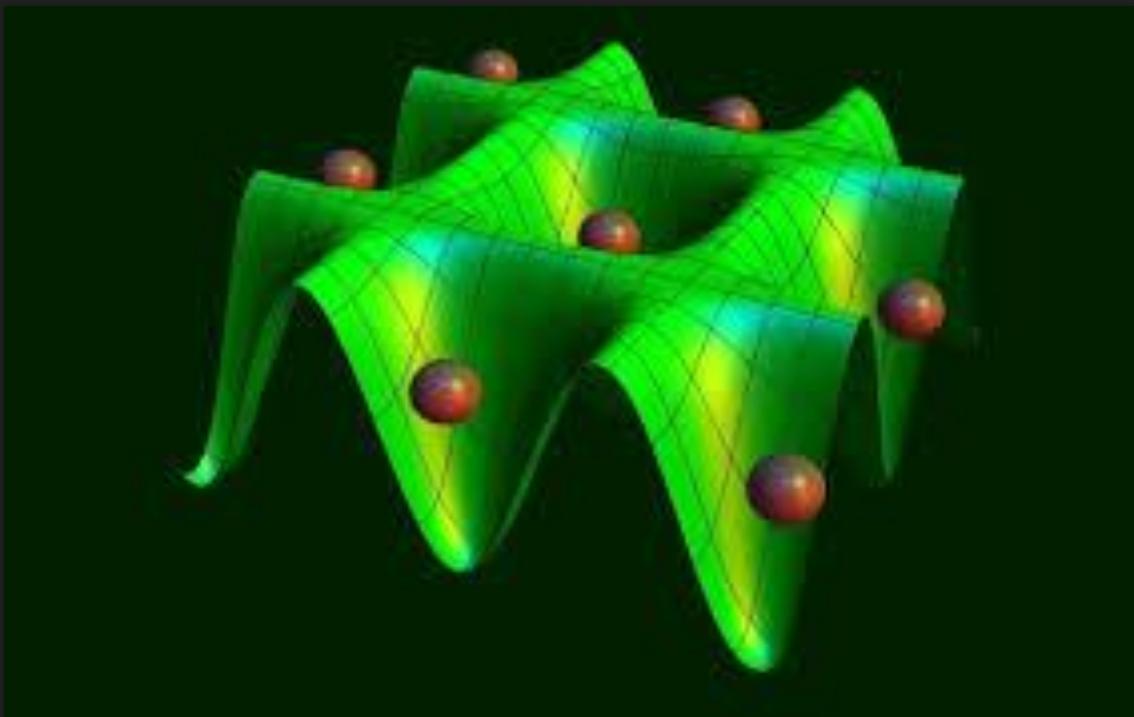
Surpreendentemente, alcançar estas temperaturas consome apenas 15,5 kW e ocupa apenas 10m² de área, em comparação com os milhares de kilowatts e metros quadrados exigidos por supercomputadores tradicionais.



Computadores quânticos à base de uma rede ótica

Uma rede ótica, “Optical lattice”, é formada pela interferência de feixes de laser, criando uma polarização espacial, criando assim poços de potencial. De seguida, átomos são arrefecidos de modo a condicionados num ponto de potencial mínimo. São utilizados átomos neutros em vez de íons, para evitar que eles interajam, indesejadamente, com as forças eletromagnéticas do ambiente devido à sua carga. Finalmente, é utilizado um outro grupo de lasers para controlar o estado dos átomos, os qubits, de modo a realizar as operações do computador quântico.

Imagen simulada de uma rede ótica



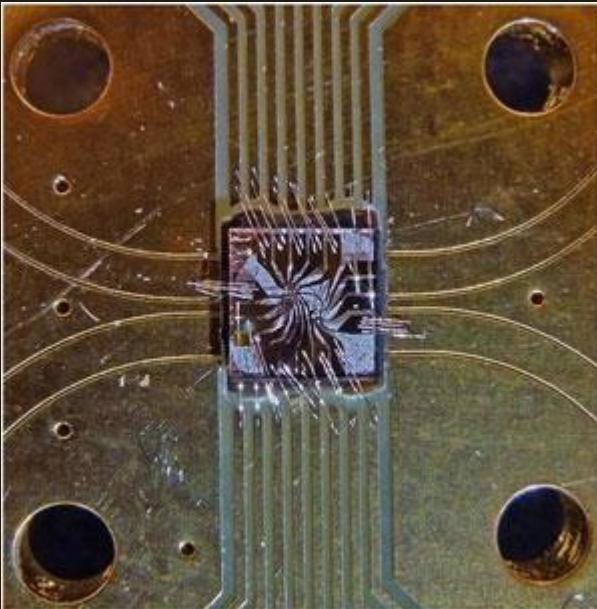
Os poços de potencial, (Verde) prendem os átomos, (castanho), como se pode ver na imagem.

Computadores quânticos à base de diamante

Os computadores quânticos à base de diamante, tiram partido de uma propriedade dos diamantes chamada “Nitrogen-vacancy center”, isto é um dos pontos de defeito do diamante, onde o átomo de carbono foi substituído por um átomo de nitrogénio e por um elétrons.

O estado dos qubits pode ser controlado através de impulsos de microondas e o facto de se encontrar dentro do diamante, fornece-lhe uma certa proteção contra o ruído externo que causaria decoerência quântica.

Computador Quântico á base de diamante



O circuito com o computador quântico à base de diamante no centro, com apenas 1mm^2 de área

Aplicações

- A construção de computadores que sejam tão pequenos a ponto de não serem visíveis a olho nu
- Simulação de física quântica
- Resolução de problemas NP-Completos
- Busca em Listas Desordenadas - O algoritmo de Grover
- Protocolo de Comunicação Segurança
- Fatoração de Números Inteiros Grandes – O algoritmo de Shor

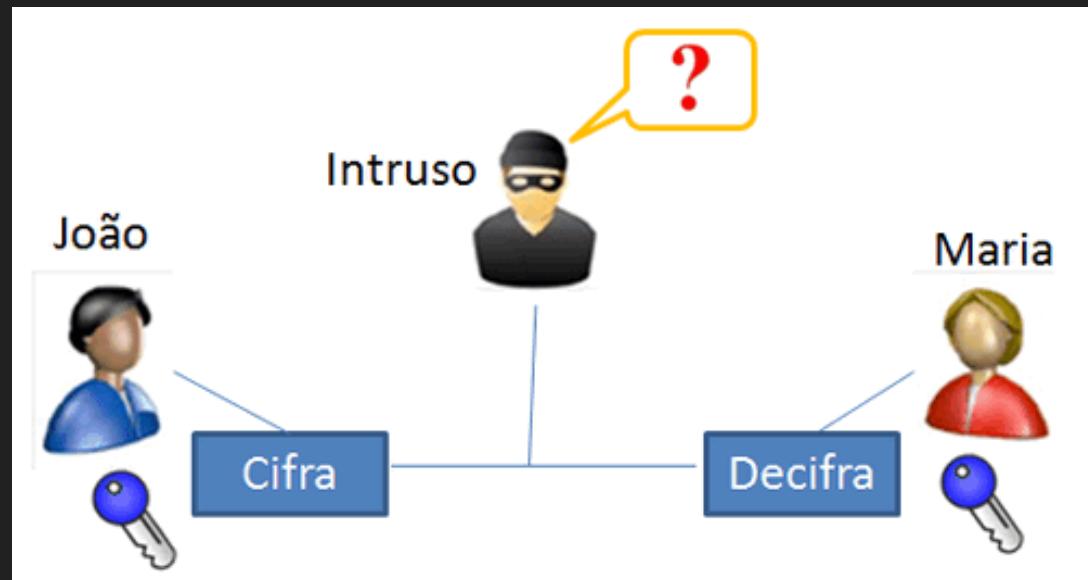
Breve introdução ao algoritmo de SHOR

- A necessidade de enviar e receber mensagens sem que outras pessoas saibam sempre existiu.
 - Um dos meios mais pensados é atribuir a cada letra um numero.
 - A = 1
 - B = 2
 - C = 3
- Porem, é necessário que tanto o remetente quanto o destinatário conheçam a tabela de códigos usados.



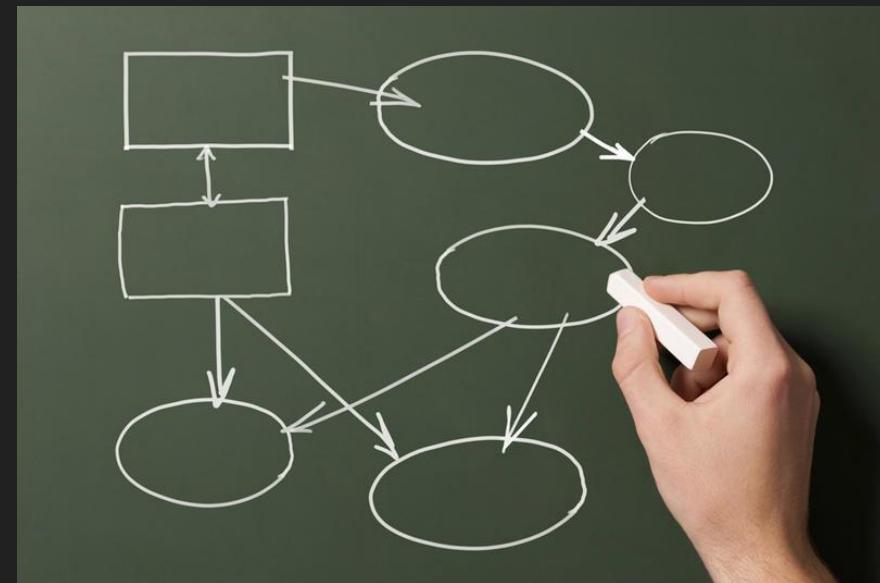
Breve introdução a criptografia

- A criptografia na qual apenas o destinatário e o remetente sabem os códigos de codificar é chamado de criptografia de chave privada.
- Já na criptografia de chave pública, todos sabem codificar, mas apenas o destinatário sabe decodificar.



Breve introdução ao RSA

- Criado no MIT.
- RSA é baseado na criptografia de chave publica.
- Sua segurança é ótima pois ainda não existe um algoritmo rápido para fatorar números compostos grandes na computação convencional.



Introdução ao Algoritmo de SHOR

- Até 1990, computação quântica era apenas uma curiosidade.
- Em 1994, Peter Shor publicou seu algoritmo quântico que resolve o problema de fatoração de números.
- Ficou conhecido como “killer application” pelo problema que poderia gerar ao RSA.
- Despertou interesse na comunidade científica.



Eficiência do Algoritmo

Tamanho do Número a Ser Fatorado (em bits)	Tempo de Fatoração por Algoritmo Clássico	Tempo de Fatoração por Algoritmo Quântico
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quadrilhões de anos	4,8 horas

Tabela 1: Comparação entre os tempos estimados para fatoração de números de tamanhos diferentes com o algoritmo clássico e com o de Shor. Fonte: Revista Ciência Hoje, Vol. 33, n. 193, Maio de 2003.

- Um computador convencional precisaria rodar por bilhões de anos para fatorar um número de 400 dígitos. Uma máquina quântica pode fazer isso em cerca de 1 ano. Códigos antes que eram indecifráveis agora poderiam ser decifrados.

Teorias para melhor compreensão

DIVISIBILIDADE

- Existem infinitos números primos.
- Dado um número $n > 1$ dizemos que n é primo se os únicos divisores de n são 1 e n .

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}^1;$$

ARITMÉTICA MODULAR

O – acima do numero diz que é representado um conjunto. Como em \mathbb{Z}_2 , são representados no conjunto 0 números pares, como -4, -2, 0, 2, 4.

OPERAÇÕES COM ARITMÉTICA MODULAR

O SOMA

$$\bar{0} + \bar{0} = \bar{0},$$

$$\bar{1} + \bar{1} = \bar{0},$$

$$\bar{1} + \bar{0} = \bar{1},$$

$$\bar{0} + \bar{1} = \bar{1}.$$

O MULTIPLICAÇÃO

$$\bar{2} \cdot \bar{0} = \bar{0}$$

$$\bar{2} \cdot \bar{1} = \bar{2}$$

$$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$$

Conjunto possui 0, 1, 2, 3, ou seja,

vai até $n - 1$ o conjunto Z_4

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{2},$$

Na soma o conjunto 0 é o elemento nulo, enquanto na multiplicação, o conjunto 1 é o elemento nulo.

Também é necessário relembrar da propriedade dos grupos.

Algoritmo de SHOR

- O algoritmo baseado em:
 - Redução do problema da busca de um fator de n .
 - Problema da busca do período de uma sequência.
- Dado um inteiro n retorna um fator do mesmo.
 - n deve ser composto ímpar.
 - n não deve ser potência de primo.

Problema: dado um inteiro positivo N , achar os fatores primos de N .

Quocientes	Divisores Primos
180	2
90	2
45	3
15	3
5	3
1	5

$180 = 2^2 \times 3^2 \times 5$

Algoritmo *Shor*(n)

1. escolha um inteiro $1 < x < n$ aleatoriamente
2. se $\text{mdc}(x, n) > 1$
3. então devolva $\text{mdc}(x, n)$
4. seja r o período da função $f(a) := x^a \text{ mod } n$
5. se r for ímpar ou $x^{\frac{r}{2}} \equiv -1 \pmod{n}$
6. então o procedimento falhou (deve-se escolher outro x e recomeçar o procedimento)
7. devolva $\text{mdc}(x^{\frac{r}{2}} + 1, n)$

- O algoritmo de Shor utiliza um único passo quântico, o 4º passo.
- Caso o algoritmo execute a linha 3, o valor é um fator de n .
- Se $\text{mdc}(x, n) = 1$, x já está em \mathbb{Z}_n^* (é um grupo com a operação produto).
- O valor da linha 7 é um fator de n .

1. Escolha um inteiro $1 < x < n$

- Queremos encontrar os fatores primos de $n = 15$.
- Escolhe-se um numero aleatório $x < n$, como $x = 7$ (notando que x não tem fatores comuns a não ser 1).

- $n = 15$
- $x = 7$
- $1 < 7 < 15$

2. Se $mdc(x, n) > 1$

3. Devolva o $mdc(x, n)$

- O $mdc(7, 15)$ deve ser calculado utilizando o algoritmo de Euclides.
- O $mdc(7, 15)$ é igual a 1. Já que não é maior que 1, pulamos o passo 3.

Entrada: números inteiros positivos distintos a e b

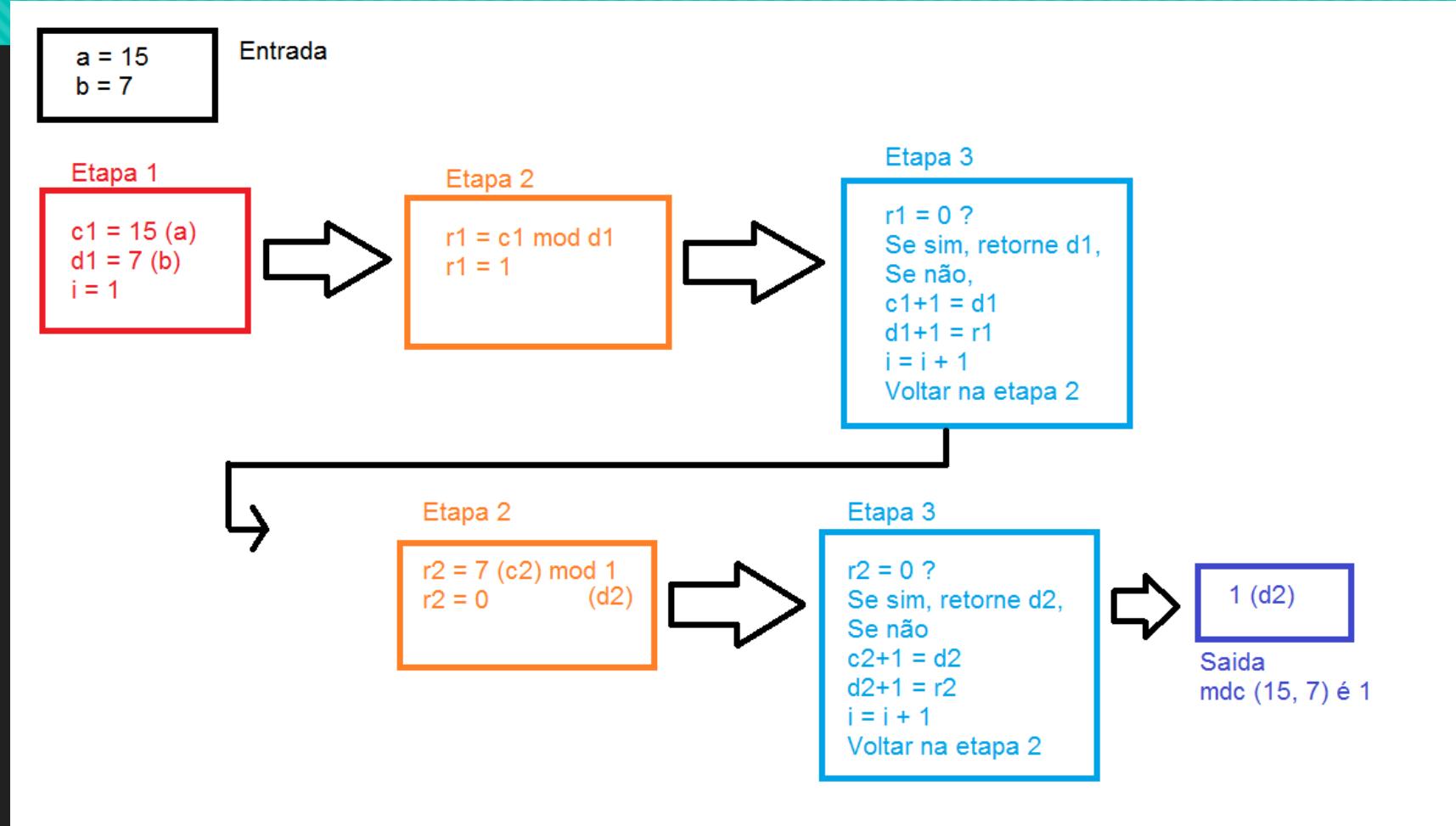
Saída: $mdc(a, b)$

Etapa 1: Comece fazendo $c_1 = a$, $d_1 = b$ e $i = 1$

Etapa 2: utilize o algoritmo da divisão para dividir c_i por d_i e retornar r_i .

Etapa 3: Se $r_i = 0$ retorne d_i , caso contrário faça $c_{i+1} = d_i$, $d_{i+1} = r_i$, acrecente 1 ao contador i e volte a etapa 2.

Teste de mesa do algoritmo de Euclides



- Note que ao envez de $\text{mdc} (15, 7)$ fizemos o $\text{mdc} (7, 15)$,

- 4. Seja r o período da função $f(a) := x^a \text{ mod } n$**
- 5. Se r for ímpar ou $x^{r/2} \equiv -1 \pmod{n}$**
- 6. Então o procedimento falhou (deve-se escolher outro x e recomeçar o procedimento.)**

O A função obtida é $f(a) = 7^a \text{ mod } 15$. O período da função f é $r = 4$ (note que f(a) assume os valores 1, 7, 4, 13, 1, 7, 4, 13... Quando $a = 0, 1, 2, 3, 4, 5, 6, \dots$). Como r não é ímpar ou $7^{r/2}$ não é identicamente igual a -1 (mod n), o procedimento não falhou, logo, a linha 6 não é executada.

7. Devolva $\text{mdc} (x^{\frac{r}{2}} + 1, n)$

- $\text{Mdc} (7^{4/2} + 1, 15) = 5$
- O valor 5 é um dos fatores primos de 15.

	3	3
50	15	5
5	0	

Sub-rotina para encontrar período

- Q-bit são uma combinação linear nos estados $|0\rangle$ e $|1\rangle$.
- Um vetor em um espaço complexo é descrito como $|\psi\rangle$ (ket psi).
- O elemento 0 é usado para denotar a origem.
- A porta de Hadamard transforma $|0\rangle$ em $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
- Ela também transforma $|1\rangle$ em $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Uma porta de 2 bits é uma porta CNOT

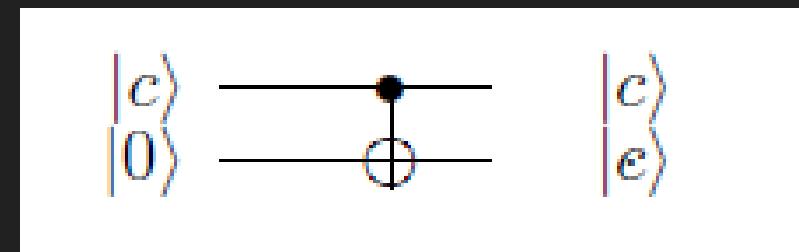
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- A porta de hadamard tem dois q-bits de entrada, um de controle e outro de alvo.
- Se o q-bit de controle for $|0\rangle$ nada acontece com o alvo.
- Se o q-bit de controle for $|1\rangle$ o q-bit alvo troca de estado.
- O q-bit de controle é o primeiro q-bit.

$$|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |10\rangle.$$

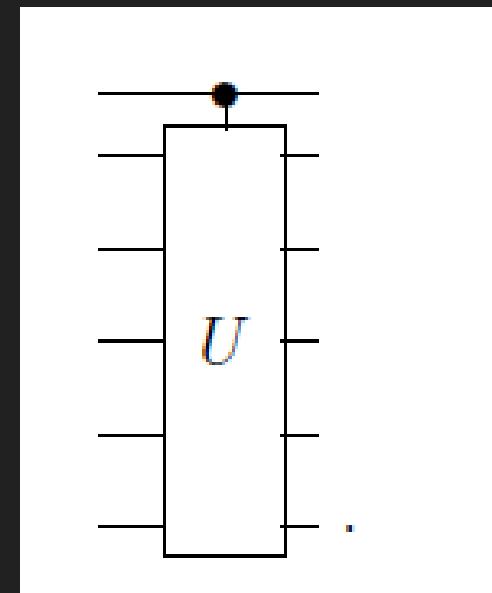
Portas lógicas

- Um circuito sempre deve ser lido da esquerda para direita.
- A porta CNOT pode copiar o q-bit de controle para o q-bit alvo (desde que o q-bit de controle seja um estado da base computacional e o q-bit alvo esteja no estado $|0\rangle$).

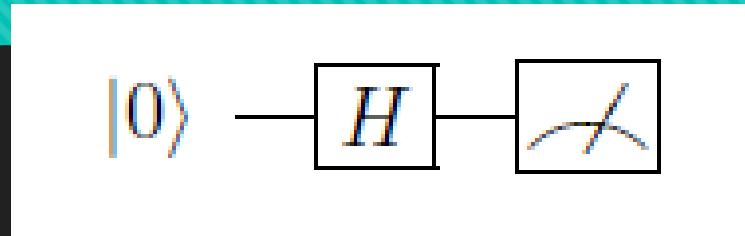


Porta Lógica U Controlada

- Atua em n-q-bits.
- Realiza operações que envolvem $n + 1$ q-bits.
- O primeiro q-bit é de controle e o resto são alvos, ou seja, q-bits nas quais a porta U atua.
- Se o q-bit de controle for 0, a porta U não será aplicada aos q-bit alvo. Se for 1 a porta será aplicada.
- É apenas uma porta CNOT generalizada para muitos q-bits.

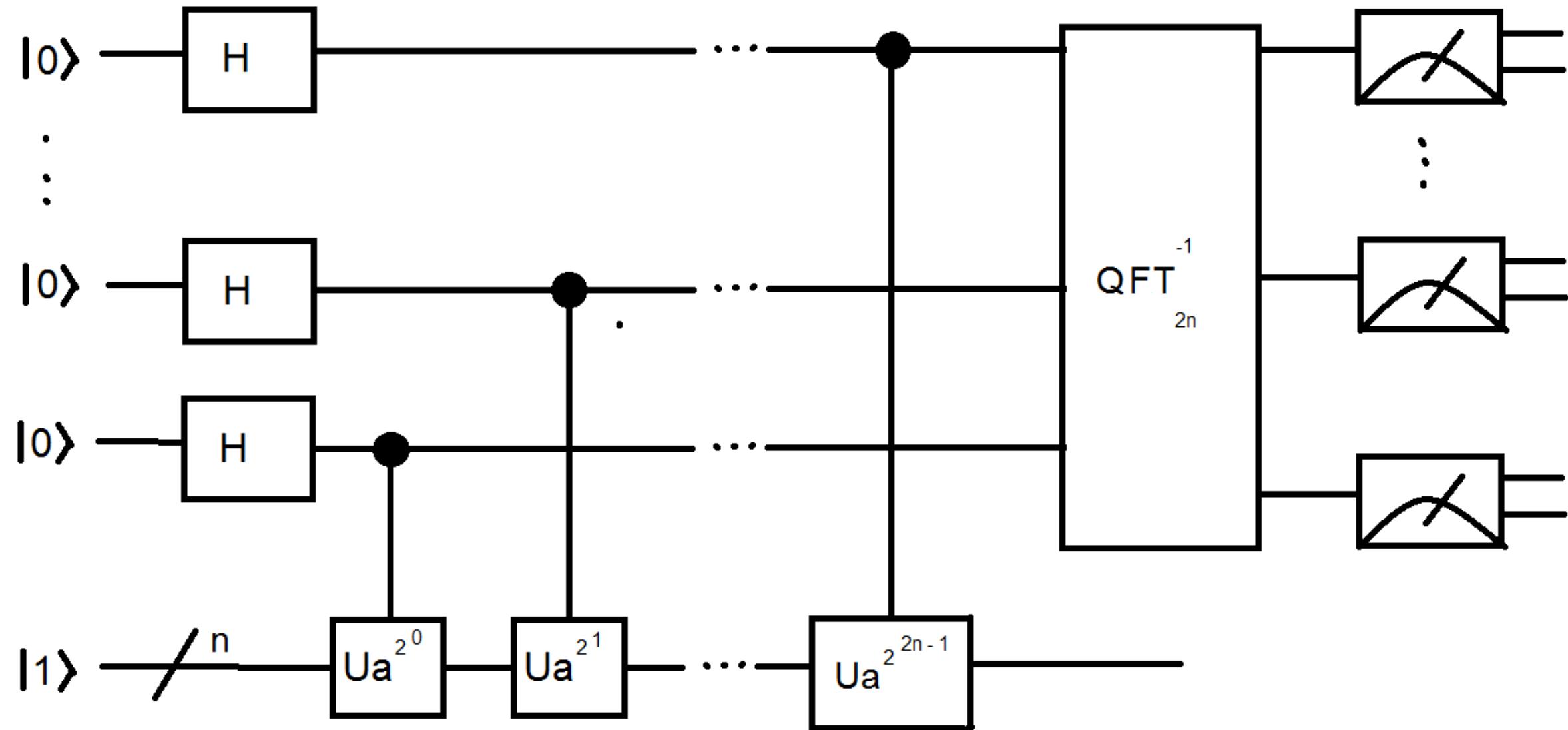


Mais alguns circuitos



- O símbolo indica que nesse estágio do circuito ocorrerá uma medição na base computacional.
- O circuito acima inicia no estado $|0\rangle$ e depois passa pela porta de Hadamard e então o estado passará a ser descrito por $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Então no final será feita uma medição na base computacional. Após a medição a probabilidade é de 50% do sistema ir para o estado $|0\rangle$ e 50% no estado $|1\rangle$.

Sub-rotina quântica no algoritmo de SHOR



Quantum Fourier Transform

- Uma das razões da velocidade do algoritmo de SHOR.
- É possível estimar estados utilizando o QFT.

Crédito

- BÁRBARA OLIVEIRA
- JOSÉ CLAUDIO ALVAREZ JUNIOR
- RAMON LACAVA GUTIERREZ GONÇALES
- MARIANA GODOY VAZQUEZ MIANO por despertar nosso interesse na área.