Computação Quântica e Criptografia

Sumário

- Introdução à criptografia
- Breve introdução à QC
- Tipos de criptografia
- Criptografia Simétrica
  - Cifra de césar
- Criptografia Assimétrica
  - RSA
- Função de Hash Criptográfica
  - SHA-3

Criptografia

Caso prático:

“Suponha que eu e você trocamos mensagem por uma rede social.
Estas mensagens não podem ser vazadas ou lidas por alguém além de nós, para isso utilizaremos criptografia, onde um terceiro sem permissão não poderia ler as mensagens, mesmo que as interceptassem no meio do caminho. ”

Cifra de césar

Uma forma de “mascarar” esta mensagem é a cifra de césar.
Ela consiste em deslocar cada letra contida na frase k letras a frente no alfabeto.
EX:
para k =1;
ola => pmb
k=2
ola => qnc

Tipos

- Simétrica
- Assimétrica
- Função de Hash Criptográfica

Hash

Utiliza funções de hash criptográficas

A partir de uma função criptografica de hash, ocorre uma série de processamentos e operações bitwise nos dados, que retornam um hash(código) para a mensagem de input.

Podem ocorrer colisões

Dependendo do algoritmo, a probabilidade de ocorrer colisões pode ser maior ou menor. Porém uma vez que um algoritmo específico foi comprometido, todas os projetos que usam ele tambem serão.

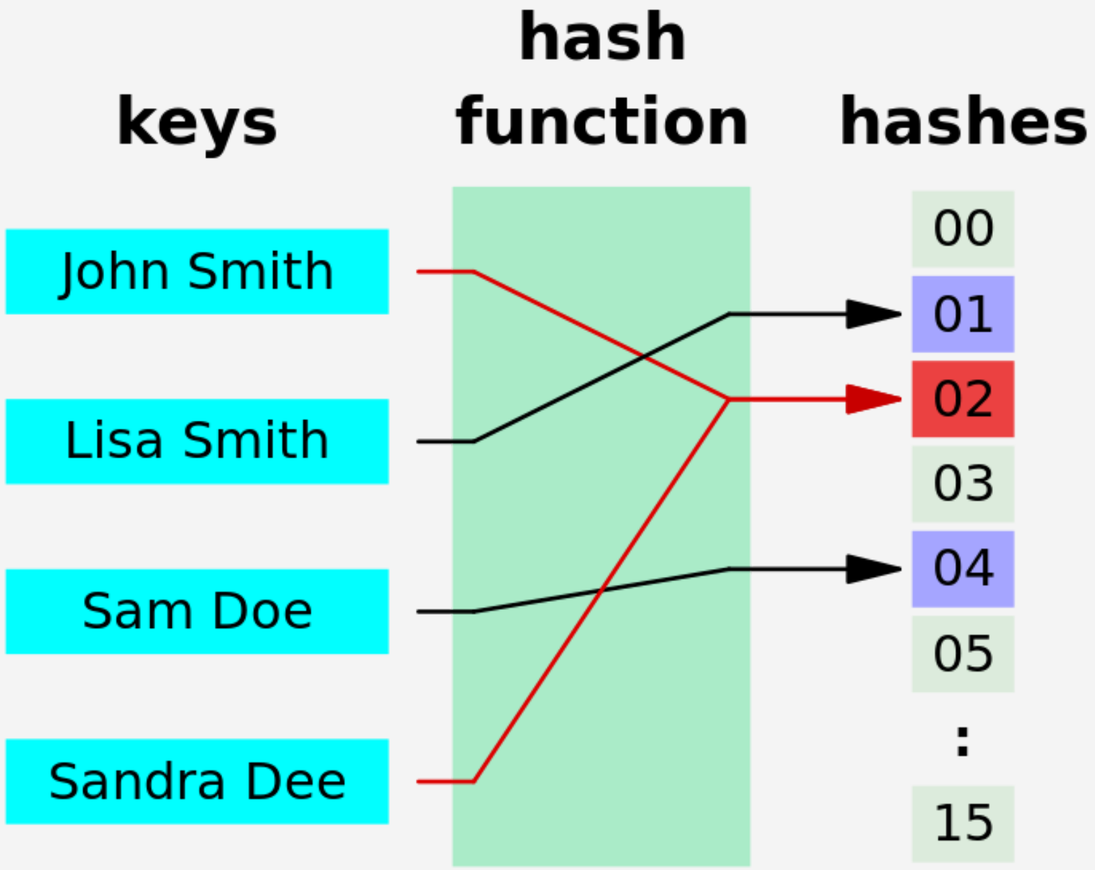
Garantem a integridade da Mensagem

A função de hash produz um unico hash para o mesmo input, porém caso ocorra uma alteração minima que seja, o hash gerado será completamente diferente. Assim podendo conferir integridade aos dados submetidos a ela.

Exemplos de Colisão

Quando dois inputs diferentes resultam no mesmo Hash, ocorre uma colisão.

Um sistema seguro deve ser resistente a colisões, com probabilidades muito baixas de ocorrência.



Simétrica

Chave é compartilhada

A chave que cifra um dado é a mesma que descriptografa

É eficiente

Tem menos custo computacional e caso alguma chave se perca é possivel somente criar outra.

Segurança baseada na chave compartilhada

Caso a chave for interceptada, todas as informações ficarão desprotegidas.

Assimétrica

Chave pública e privada

A chave pública é utilizada para cifrar uma mensagem, já a privada é utilizada para decifra-la. Para enviar algo, precisa-se apenas a chave publica do destinatario que usara uma chave privada para decifrar

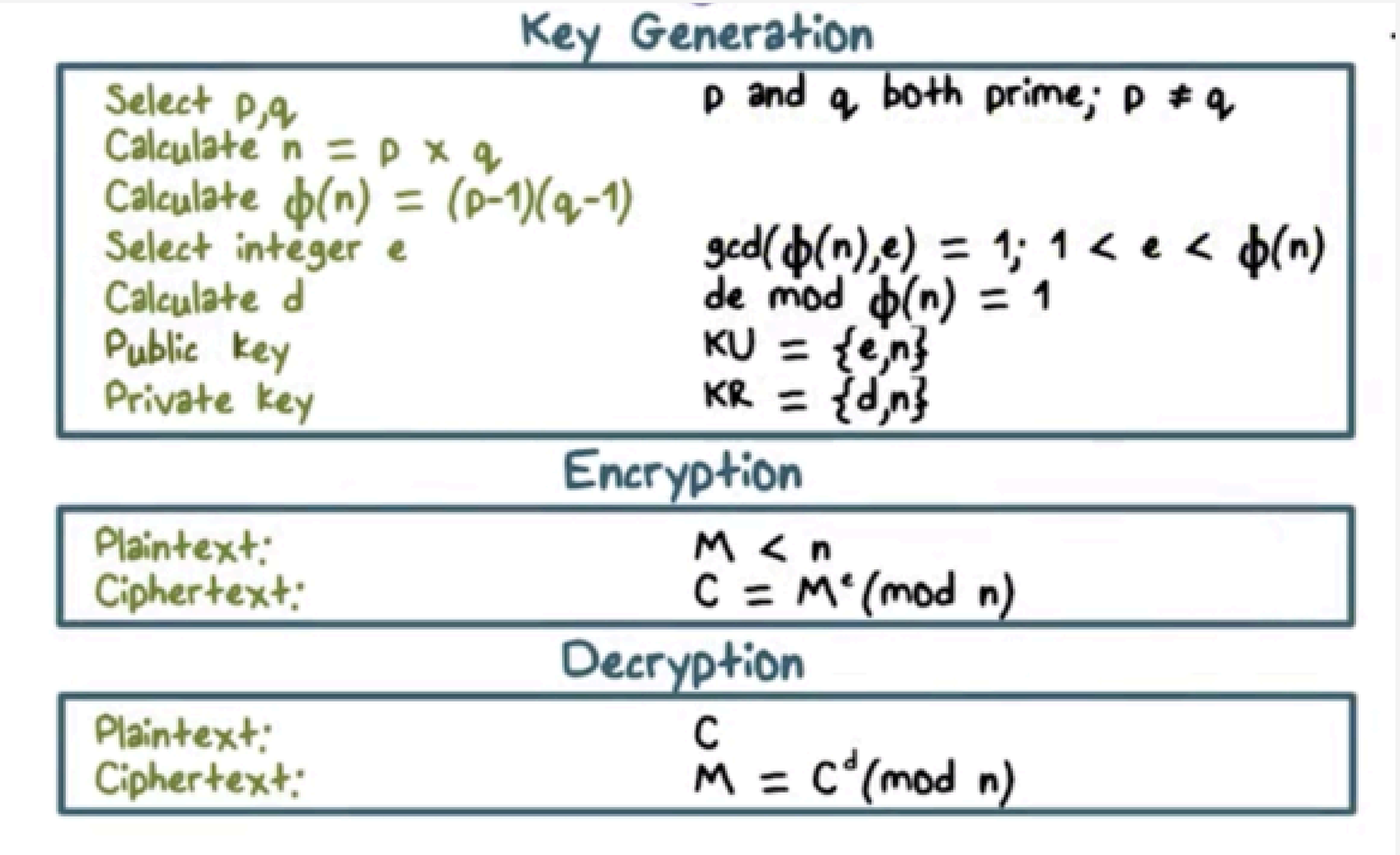
Mais custosa

Tem calculos complexos envlvidos na construção das chaves,

Segurança baseada na chave privada de um único dono

Caso a chave for interceptada, todas as informações ficarão desprotegidas.

Exemplo: RSA


Key Generation
Select p,q
p and q both prime; p ≠ q
Calculate n = p x q
Calculate ϕ(n) = (p-1)(q-1)
Select integer e
gcd(ϕ(n),e) = 1; 1 < e < ϕ(n)
Calculate d
de mod ϕ(n) = 1
Public key
KU = {e,n}
Private key
KR = {d,n}
Encryption
Plaintext:
M < n
Ciphertext:
C = M^e (mod n)
Decryption
Plaintext:
C
Ciphertext:
M = C^d (mod n)

Pequeno desafio

Achem 2 números primos P e Q que resultem em 22

Dificultando um pouco...

Fatorem o número 2024 em 2 primos
Q e B

Ficando impossível!

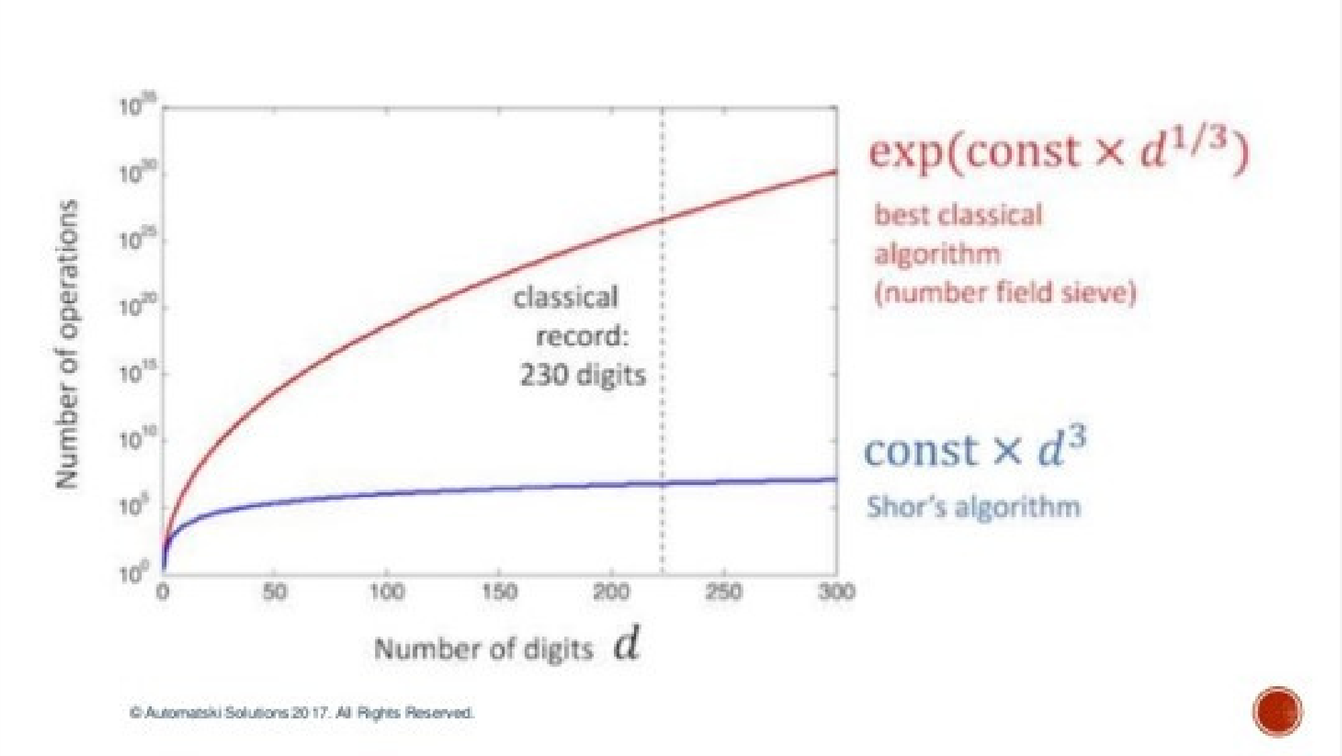
Para finalizar fatorem o número 2^2048 em 2 primos Q e B

Ficou dificil, não?

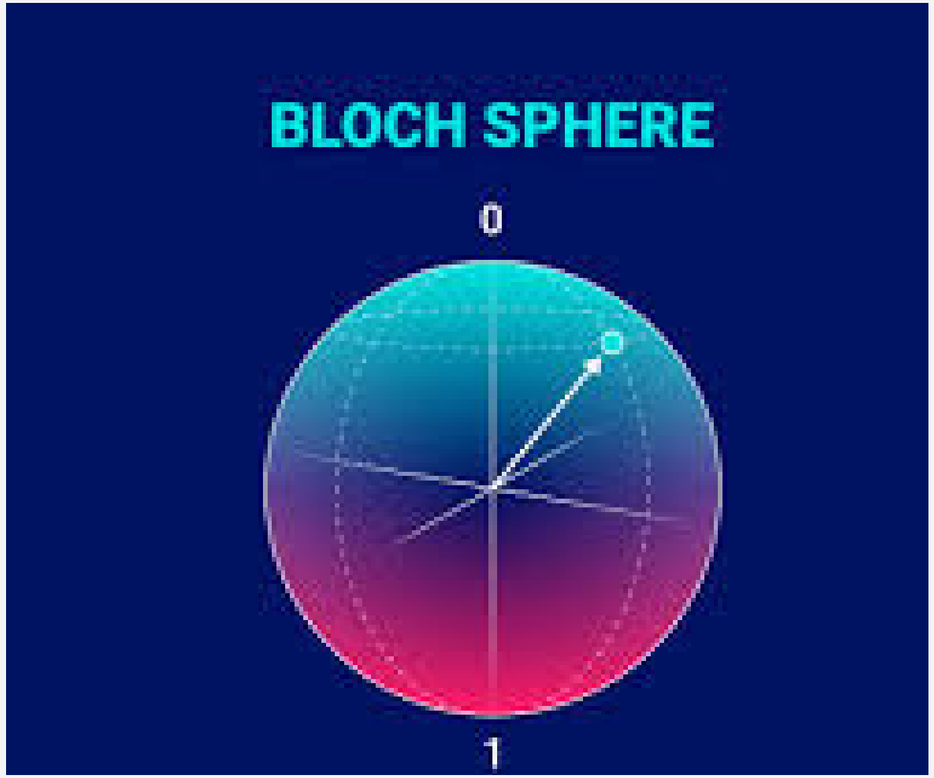
Problema da fatoração

A complexidade é da ordem de O(exp(n))
onde n é o número de dígitos do número a ser fatorado.

Isso é um dos motivos para a segurança do RSA



Computação quântica

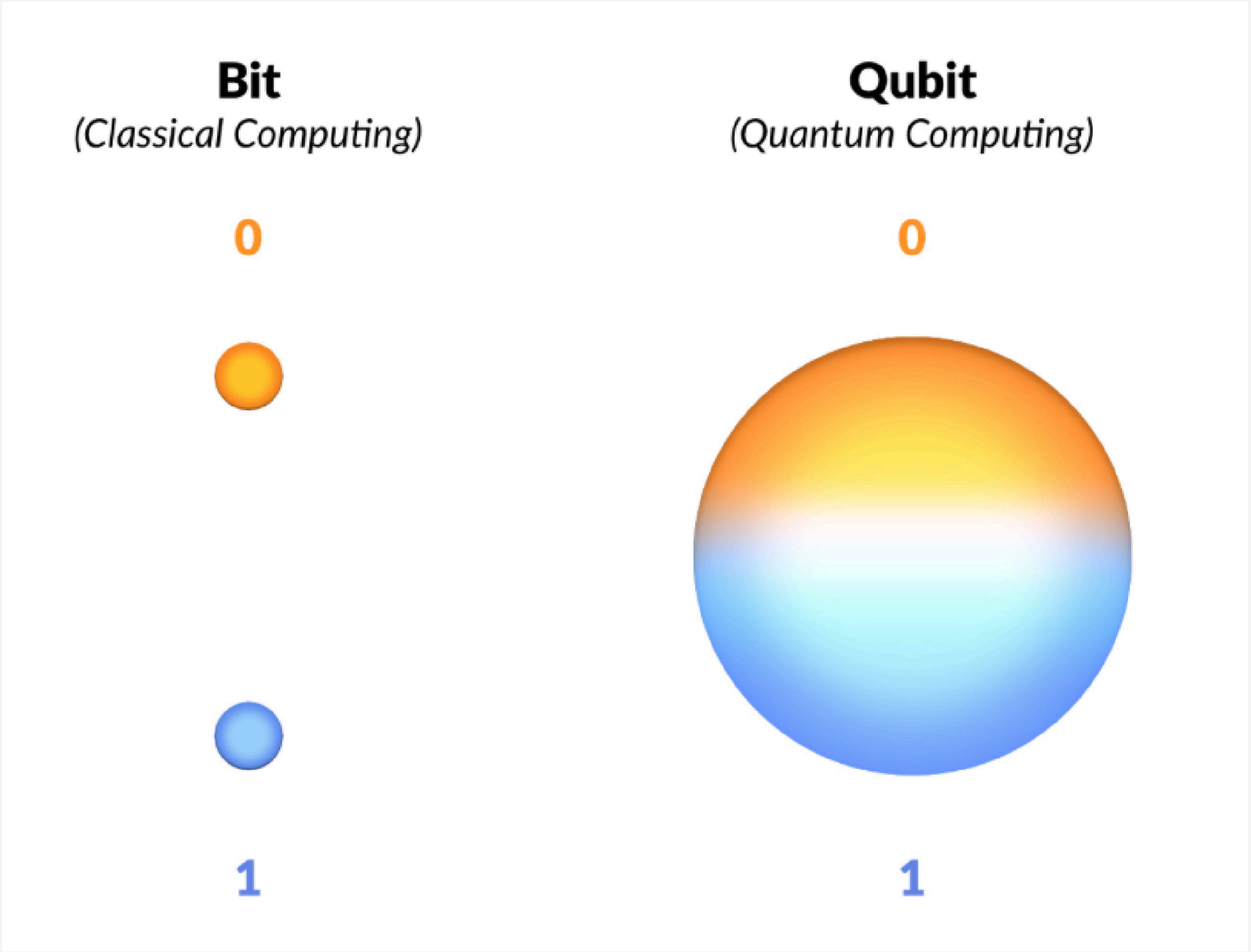


Na computação quântica usamos de fenômenos quânticos como a superposição e o entrelaçamento para conseguirmos resolver problemas que computadores clássicos não conseguem resolver de maneira eficiente.

Bit vs Qubit

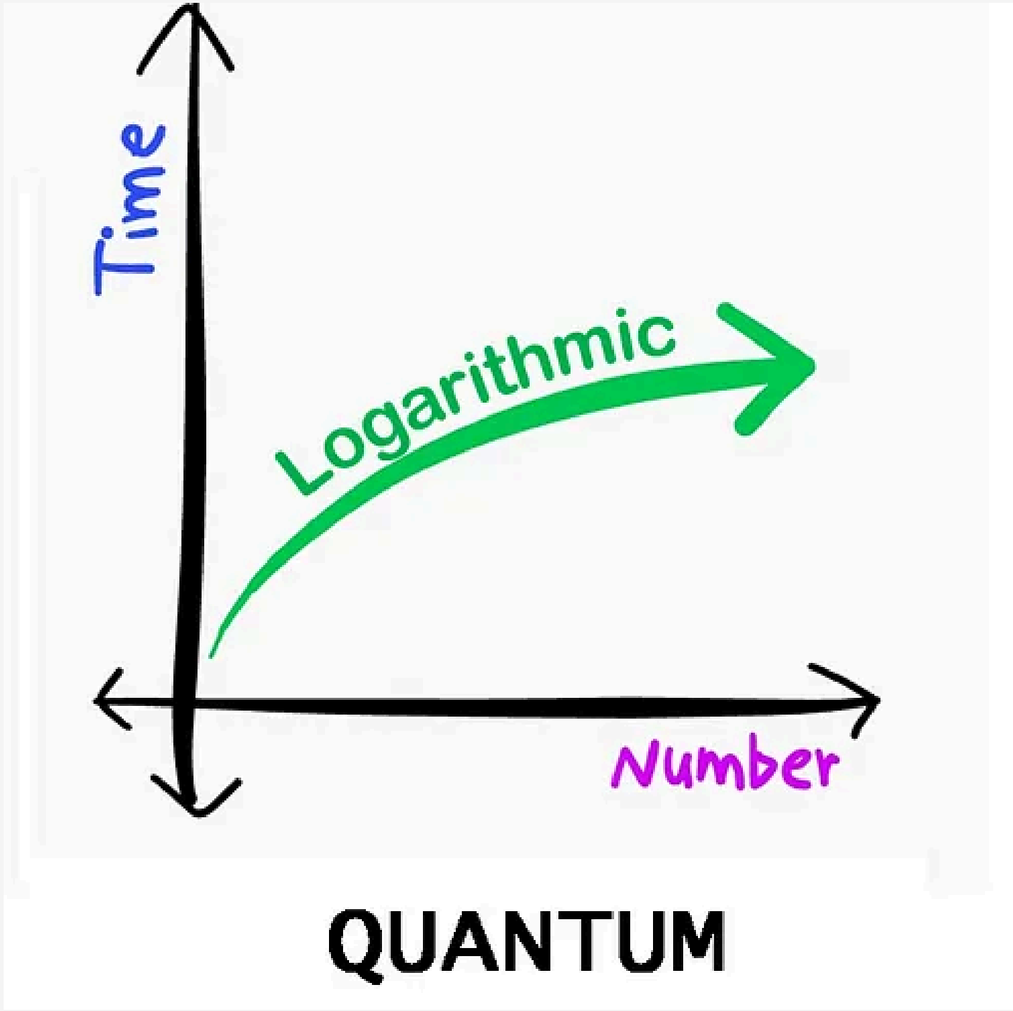
O Bit apresenta apenas um estado ao mesmo tempo, já o qubit pode apresentar uma superposição de estado.

Esta diferença traz vantagens ao qubit que pode processar mais informações ao mesmo tempo, tendo um paralelismo intrínseco e a possibilidade de novos algoritmos



Algoritmo de Shor

O algoritmo de shor utiliza a computação quântica para encontrar o período da função aplicada no algoritmo testando múltiplos candidatos que serão a chave para a fatoração



Novo padrão NIST

Projetos de Criptografia Pós-Quântica para padronizar algoritmos criptográficos seguros contra ataques de computadores quânticos.

Para saber mais

Simétrica

DES

Exemplo

AES

Exemplo

Cifra de césar

Exemplo

Assimétrica

RSA

Exemplo

Hash

SHA-3

Exemplo

Keccak-256

Exemplo

Kahoot

Falhas e alternativas

Distribuição de chaves

- Utilizar criptografia assimétrica

Resistência a ataques

- Aumentar o comprimento das chaves
- Utilizar padrões do NIST
- Utilizar algoritmos mais robustos como o AES

Integridade e confiabilidade

- Utilizar MACs para autenticação e integridade da mensagem

Segurança da chave

- Trocar de chave regularmente
- Utilizar sistemas de armazenamento seguros