Alice, Bob and Eve – Quantum Cryptography

Hands on Quantum Mechanics

João Sabino

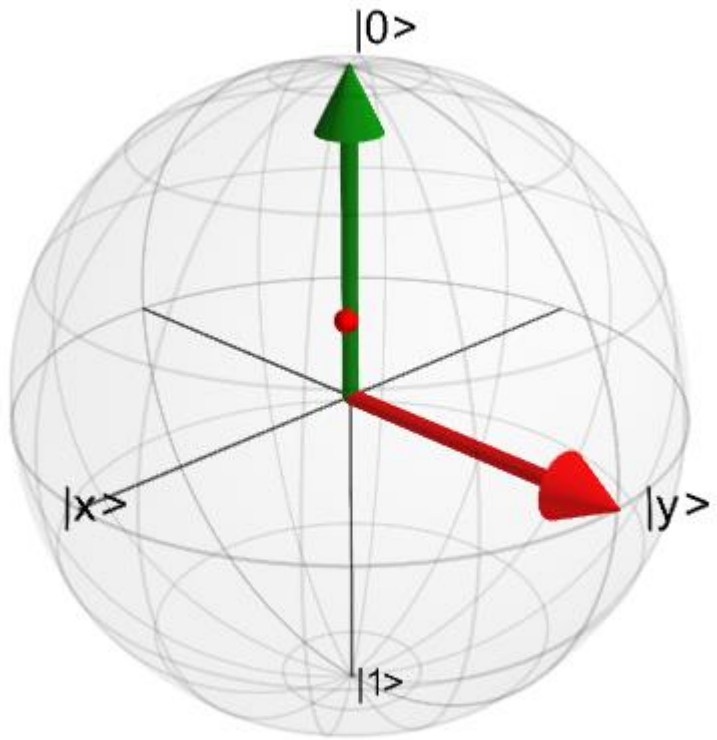
Payback time – The Bloch Sphere

A forma geral de um Qubit é:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$

No entanto, o factor γ da fase não tem significado físico, portanto, todos os estados que apenas diferem na fase, são representados pelo mesmo ponto.

Em particular, os eixos representam, grosso modo, as grandezas que se medem.



Bell States

Estes são os estados que nos permitem concretizar sistemas de criptografia seguros.

A propriedade essencial é: medindo o estado de um qubit, sabe-se, instantaneamente, qual o estado do outro qubit, ainda que estes se encontrem separados por grandes distâncias.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

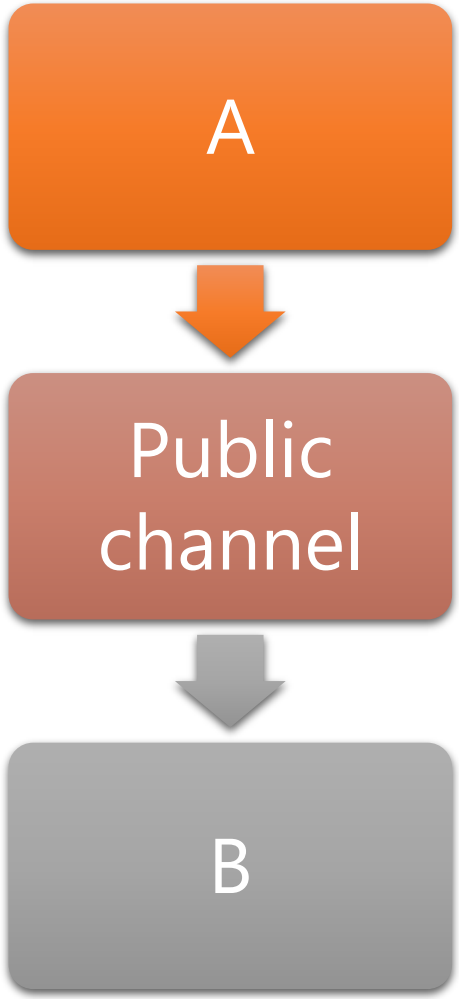
$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Criptografia

parties to achieve, with provable security, two of the main goals of cryptography: encrypting a subsequent meaningful message to make it unintelligible to a third party [1], and certifying to the legitimate receiver that a message (plain or encrypted) has not been altered in transit [2].

If two parties share no secret information initially and

O objectivo principal da Criptografia é que duas entidades diferentes comuniquem em privado.



Criptografia

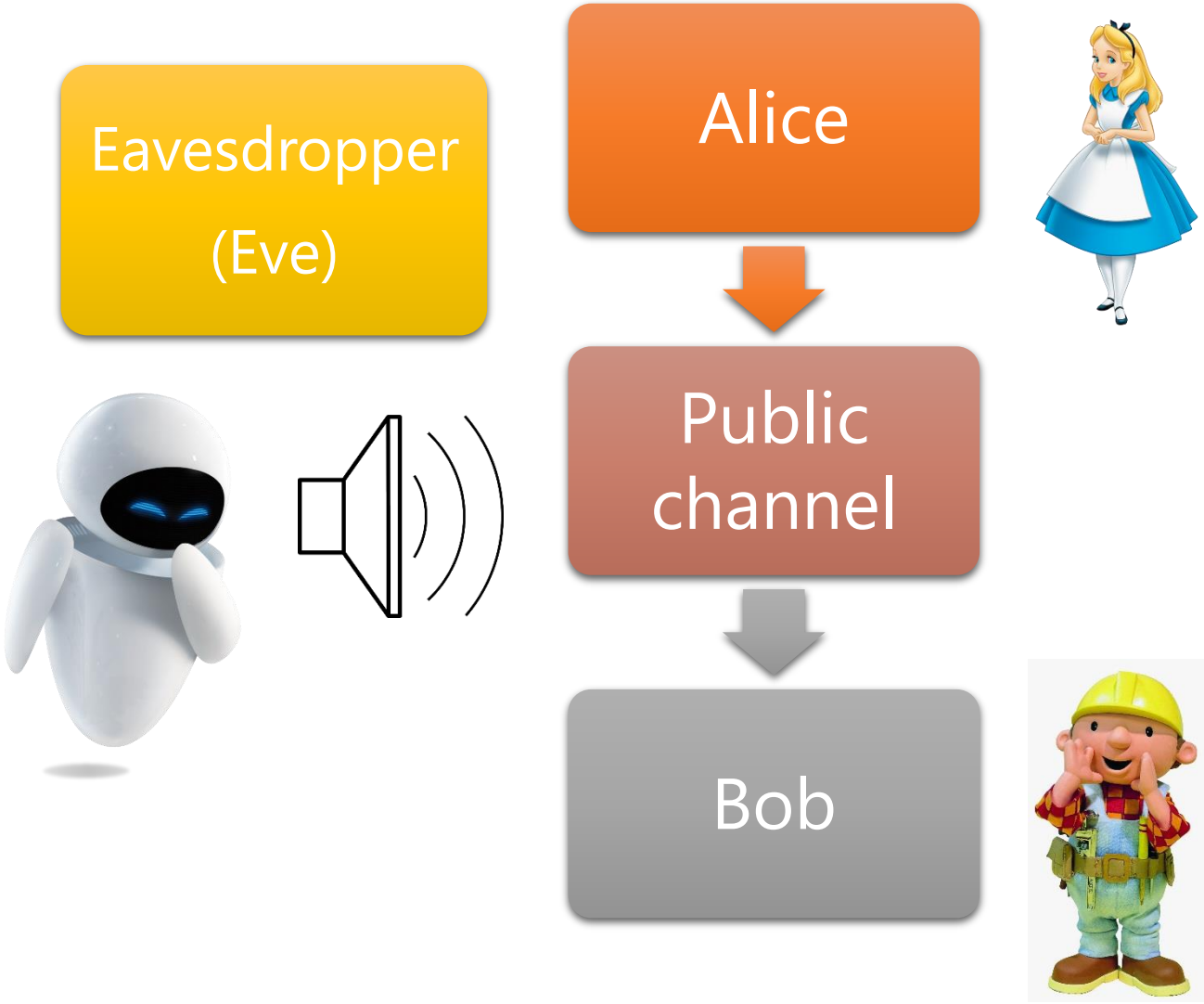
CRIPTOGRAFIA DE CHAVE PRIVADA

Apenas a Alice e o Bob conhecem a chave que pode desencriptar a mensagem.

CRIPTOGRAFIA DE CHAVE PÚBLICA

Chave pública – acessível a todos (usada para encriptar a mensagem)

Chave privada – apenas conhecida pelo Bob (receptor da mensagem a descodificar)



COMO???

Key distribution - RSA

1. Seleccionar dois números primos *p* e *q;*
2. Calcular o produto *n=pq;*
3. Escolher, aleatoriamente um inteiro *e*, de tal modo que *e* e $\varphi(n) = (p-1)(q-1)$ sejam primos entre si,
4. Calcular o multiplicativo inverso de *e*, módulo $\varphi(n)$
5. A chave pública é $P = (e, n)$ e a chave privada é $S = (d, n)$

$$E(M) = M^e (\text{mod } n)$$

$$E(M) \rightarrow D(E(M)) = E(M)^d (\text{mod } n)$$

$$\begin{aligned} D(E(M)) &= E(M)^d (\text{mod } n) \\ &= M^{ed} (\text{mod } n) \\ &= M^{1+k\varphi(n)} (\text{mod } n) \\ &= M \cdot M^{k\varphi(n)} (\text{mod } n) \\ &= M (\text{mod } n) \end{aligned}$$

QKD – Quantum key distribution

Proposition : (**Information gain implies disturbance**) In any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance to the signal.

Ou seja… Qualquer tentativa de extracção de informação pode ser detectada!

QKD – Quantum key distribution

Alguns dos protocolos mais conhecidos:

- Protocolo EPR
- Protocolo BB84
- Protocolo B92

Protocolo EPR

1. Os qubits são distribuídos no estado

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

2. As desigualdades de Bell são testadas para garantir fidelidade – coloca um limite inferior para a fidelidade dos qubits restantes

3. A Alice mede os qubits na base X ou Z aleatoriamente, obtendo o resultado a

4. O Bob faz o mesmo obtendo o resultado a'

5. As bases das medições são anunciadas

6. A chave são os pares {a,a'} cujas bases são idênticas.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Protocolo BB84

The BB84 QKD protocol

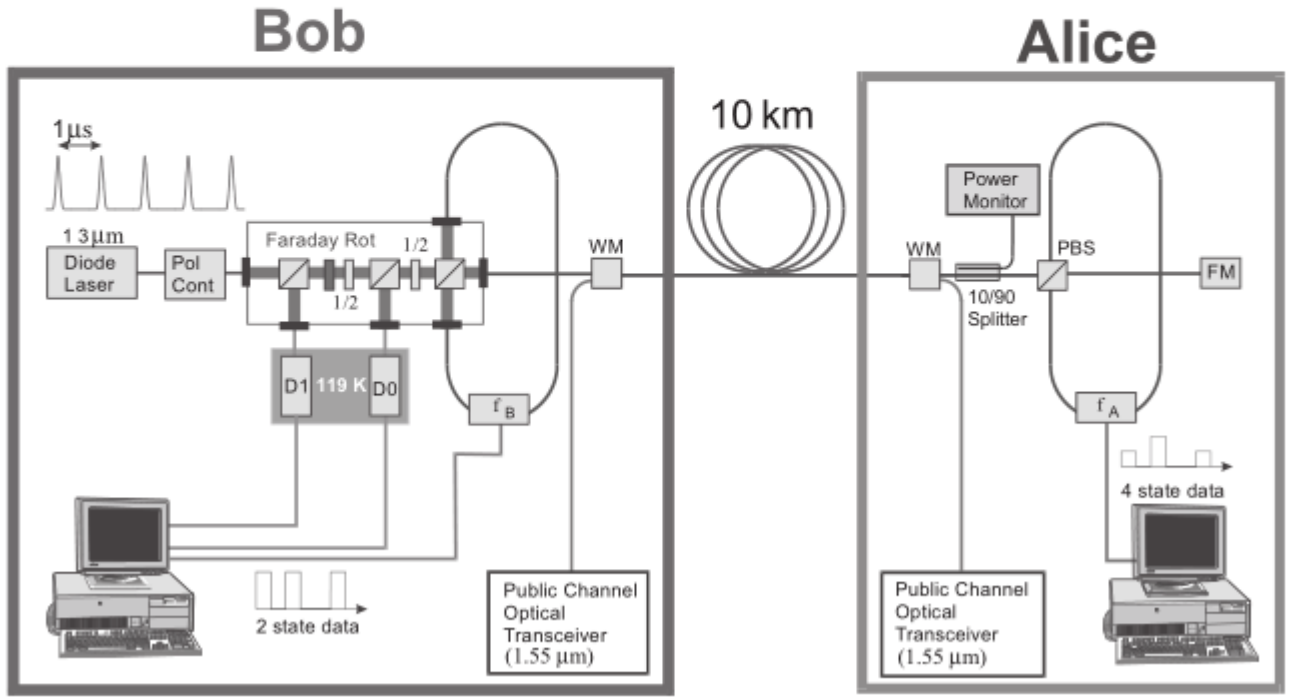
1: Alice chooses $(4 + \delta)n$ random data bits.
2: Alice chooses a random $(4 + \delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
3: Alice sends the resulting state to Bob.
4: Bob receives the $(4 + \delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
5: Alice announces b.
6: Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
7: Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8: Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9: Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

$$|\psi_{00}\rangle = |0\rangle$$
$$|\psi_{10}\rangle = |1\rangle$$
$$|\psi_{01}\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$
$$|\psi_{11}\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$$

Protocolo BB84

Box 12.7: Experimental quantum cryptography

Quantum key distribution is particularly interesting and astonishing because it is easily experimentally realized. Here is a schematic diagram of one system employing commercial fiber-optic components to deliver key bits over a ten kilometer distance, which has been built at IBM:



Protocolo B92

1. Aalice envia a informação dos bits clássicos *a* sob a forma de qubits ao Bob
2. O Bob gera o seu próprio vector de bits clássicos *a'* e mede os qubits enviados na respectiva base
3. O Bob anuncia o seu resultado *b* publicamente (mantendo *a'* em segredo)
4. Analisam-se os pares {*a*,*a'*} para os quais *b*=1
5. A chave será *a* para a Alice e 1-*a'* para o Bob

$$|\psi\rangle = \begin{cases} |0\rangle & \text{if } a = 0 \\ \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} & \text{if } a = 1 \end{cases}$$

Obrigado!

" Our field is still in its embryonic stage. It's great that we haven't been around for 2000 years. We are still at a stage where very, very important results occur in front of our eyes."

– Michael Rabin, on computer Science