

"Eu queria agradecer-te, Galileo;
a inteligência das coisas que me deste."
António Gedeão



"e de ao colapso de uma delas
uma só; a frio observada
a outra tornar-se vivo
de enlace ao colapso também"
Joana Espain

Pedra Filosofal

Eles não sabem que o sonho é uma constante da vida tão concreta e definida como outra coisa qualquer, como esta pedra cinzenta em que me sento e descanso; como este ribeiro manso; em serenos sobressaltos como estes pinheiros altos que em verde e ouro se agitam como estas aves que gritam em bebedeiras de azul. Eles não sabem que o sonho é vinho; é espuma, é fermento; bichinho álsche e sedento; de focinho pontiagudo; que fossa através de tudo num perpétuo movimento. Eles não sabem que o sonho é tela, é cor, é pincel, base, fuste, capitel, arco em ogiva, vitral, pináculo de catedral, contraponto, sinfonia, máscara grega, magia, que é retórica de alquimista, mapa do mundo distante, rosa dos ventos, Infante, caravela quinhentista, que é Cabo da Boa Esperança, ouro; canela, malfim, florite de espadachim, bastidor, passo de dança., Colombina e Arlequim, passadeira voadora, pára-raios, locomotiva, barco de proa festiva, alto-forno; geradora, cisão do átomo; radar, ultra som televisão desembarque em foguetão na superfície lunar. Eles não sabem, nem sonham, que o sonho comanda a vida. Que sempre que um homem sonha o mundo pula e avança como bola colorida entre as mãos de uma criança.

António Gedeão

Paradoxo

O presente, o meu presente, é paradoxal e já não se dá por isso. Essa não é a era da suspeita. É a era da indiferença ao paradoxo. Não sei se isto é bom ou mau. Sei que, para mim, é estranho e excitante. Mas faz medo. É como se os paradoxos da Mecânica Quântica andassem à solta pelo supermercado. E andam. Sem alarmar ninguém.

Detesto o paradoxo do gato de Schrödinger. Gosto do paradoxo de la boîte à Tokyo

Adília Lopes

La boîte à Tokyo

Aquele que a procura ainda não voltou ou porque ainda a procura ou porque já a encontrou

Adília Lopes

Pedaco 13,73

É então: entanglement como se dissesse magia delicadamente e as partículas tremessem, essas de que falas falassem também mas ainda mais baixo que tu e não fossem dissolúveis em música falassem do seu longo enlace da luz fria na pele à dança ardente no interior de uma anã gigante e de ao colapso de uma delas uma só; a frio observada a outra tornar-se vivo de enlace ao colapso também do seu segredo atravessar o universo como se um beijo fosse mais rápido que a luz e ao eco agudo desse colapso uma melodia ténue fosse sendo diminuída exatamente como o som que a informação faz ao dissolver

Joana Espain

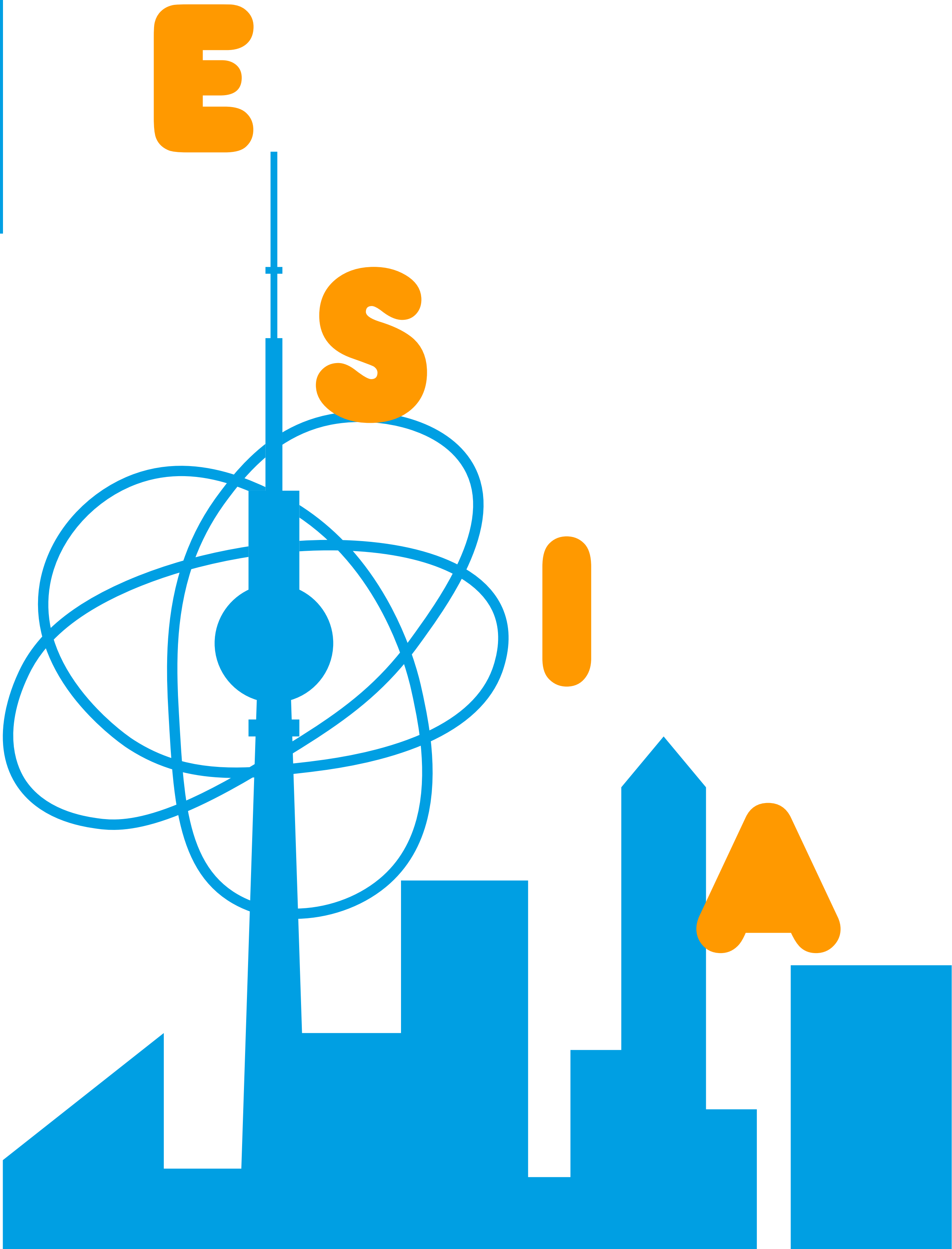
If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em.

Jennifer and Peter Shor

Esteira E Cesto

No entrançar de cestos ou de esteira
Há um saber que vive e não desterra
Como se o tecedor a si próprio se tecesse
E não entrançasse unicamente esteira e cesto

Sophia de Mello Breyner



A GRANDE REVOLTA DOS GATOS DE SCHRÖDINGER APÓS 100 ANOS DE QUÂNTICA



A GRANDE REVOLTA DOS GATOS DE SCHRÖDINGER APÓS 100 ANOS DE QUÂNTICA



O que significa o protesto destes gatos? Será um protesto contra a violência contra animais? Porque é que os cartazes dizem: "stop experimenting", "we are cats not kets", "I am not $|dead\rangle$ "?

Tudo começou com a experiência imaginária que o físico austríaco Erwin Schrödinger propôs em 1935 para explicar como os conceitos da mecânica quântica não fazem sentido no mundo que nós conhecemos. Contou então a história de um gato, o Gato de Schrödinger, e desde então os gatos nunca mais tiveram paz, vivendo com o medo constante de estarem mortos.

Imaginemos o seguinte cenário estranho: temos uma caixa fechada e, lá dentro, está um gato, um frasco de veneno e uma máquina muito especial ligada a uma partícula radioativa. A qualquer momento, a partícula pode ou não "decair" – se decair emite um pequeno sinal que ativa a máquina. Se o sinal for emitido, o frasco de veneno parte-se e o gato morre.

Enquanto o sinal não for emitido, o gato mantém-se vivo. Nós estamos fora da caixa e não sabemos se o gato está vivo ou morto. Temos de abrir a caixa para saber. Imaginemos que temos muitas caixas iguais, que foram fechadas todas ao mesmo tempo e abertas todas ao mesmo tempo. Nalgumas caixas encontramos um gato vivo e noutras um gato morto. O que diria a mecânica quântica se o gato fosse uma partícula quântica? Enquanto ninguém abrir a caixa, o gato está simultaneamente vivo e morto. Sim, lê-te bem! Como é que isto pode ser possível? Não faz sentido!



Esta experiência imaginária mostra quão estranhas são as regras da mecânica quântica, um ramo da física que estuda as partículas mais pequenas do universo. Partículas como os eletrões de que certamente já ouviste falar. Nessas escalas minúsculas, as partículas podem existir em dois estados ao mesmo tempo (ou até mais do que dois) – algo chamado sobreposição de estados. Só sabemos em que estado a partícula realmente está se fizermos uma medição. No caso do gato, enquanto não abrimos a caixa para espreitar (enquanto não fizermos a medição), ele está num estado "misto", vivo e morto ao mesmo tempo.

Claro que, na vida real, os gatos não funcionam como partículas quânticas e Schrödinger não queria que ninguém colocasse gatos em caixas! A experiência é apenas uma metáfora que nos ajuda a compreender que, no mundo quântico, as partículas comportam-se de forma que desafia o nosso senso comum.

Os cartazes no protesto brincam com esta ideia. "Stop experimenting" pede o fim de experiências hipotéticas que colocam os gatos em situações em que podem ser mortos. "We are cats, not kets" é um trocadilho com o termo "ket", um termo usado na mecânica quântica para representar estados quânticos, o estado das partículas. Já a frase "I am not $|dead\rangle$ " é uma piada sobre a notação usada na física: " $|dead\rangle$ " é a notação usada para o ket que representa o estado "morto" do gato.

No nosso mundo macroscópico, não faz qualquer sentido dizer que um objeto – ou um animal, como um gato – existe em dois estados ao mesmo tempo. A experiência do Gato Schrödinge é famosa por mostrar como é absurdo pensar no nosso mundo macroscópico como se fosse um mundo quântico. O protesto imaginário dos gatos é uma forma bem-humorada de lembrar que, por mais que a ciência avance, os gatos (felizmente!) preferem ser apenas... gatos.

Seja na ciência ou no humor, o Gato de Schrödinger continua a inspirar e desafiar a nossa forma de ver o mundo!



Autores da ilustração: Sagar Pratapsi e Joana Esteves.

Sagar Pratapsi é o autor da ideia associada à ilustração e do texto dos cartazes de protesto. É doutorado em computação quântica, professor do curso "Computação e Tecnologias Quânticas" da Universidade de Coimbra, e pertence ao grupo Quantum@UC.

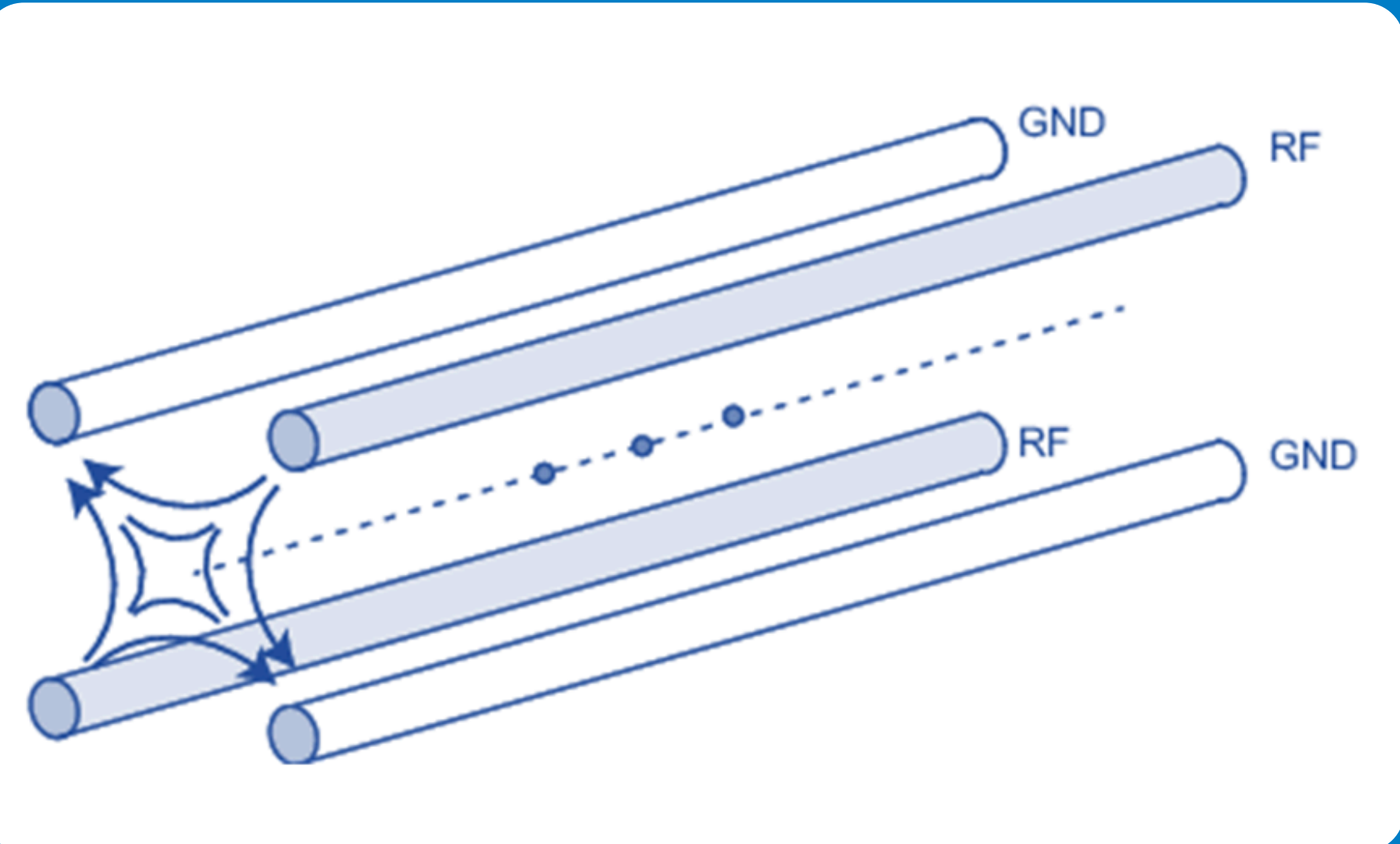
Joana Esteves ilustrou o protesto dos gatos. É uma ilustradora profissional original de Vila Real, que vive e trabalha em Coimbra. Para ver mais dos seus trabalhos, pode visitar o seu website joanaesteves.pt.

COMPUTADORES QUÂNTICOS: IÕES CONFINADOS

Sagar Pratapsi
Universidade de Coimbra

1. Iões confinados

Os **iões confinados** (trapped ions) são uma das plataformas mais promissoras para computação quântica.

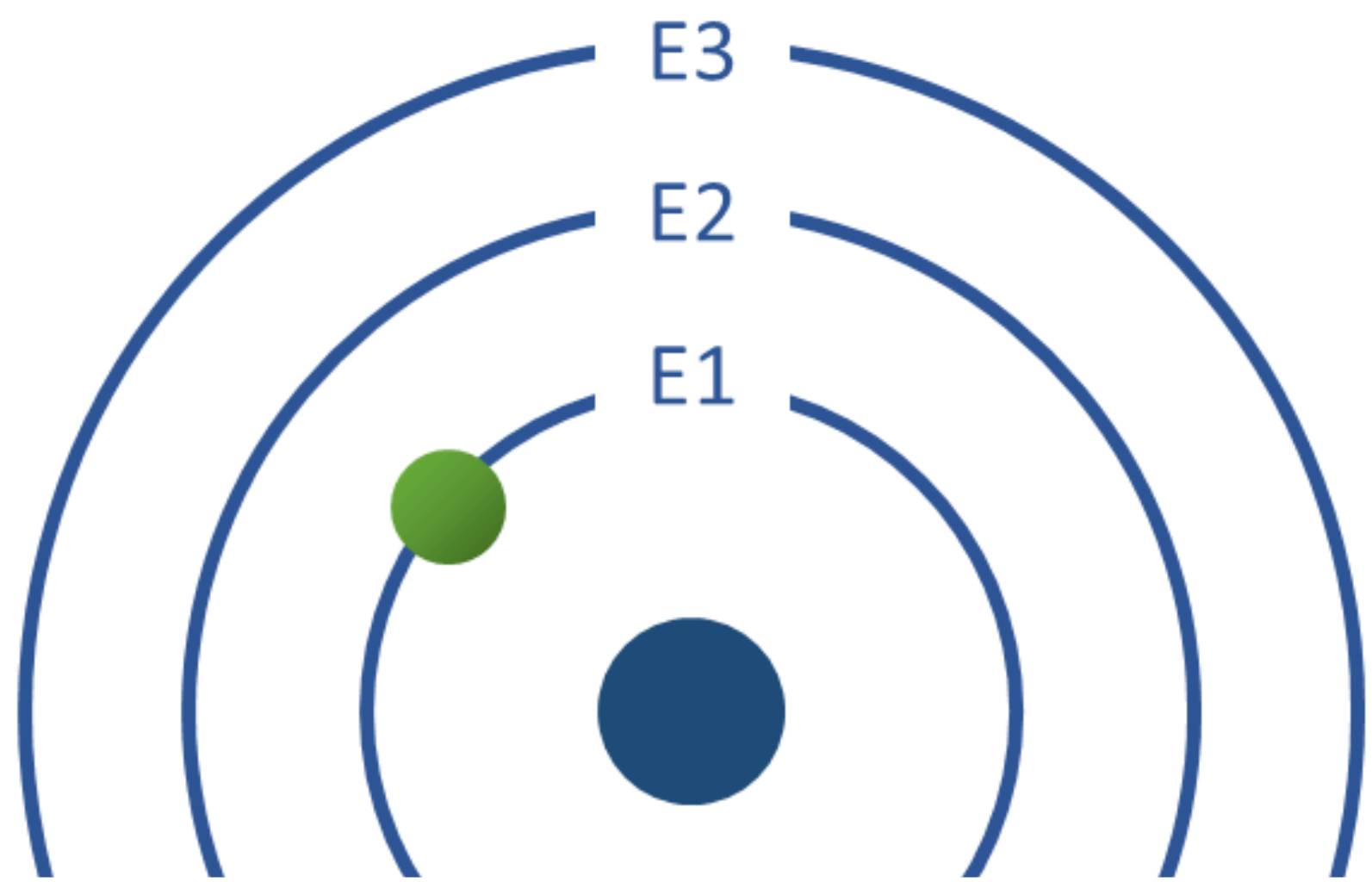


As **“Paul traps”** confinam os iões usando campos eletromagnéticos oscilantes. Tipicamente, aplica-se uma voltagem quadrupolar, como na imagem. São o método de *trapping* mais comum.

Utilizam-se dois terminais elétricos nas pontas para confinar os iões na direção longitudinal.

2. Qubits com iões

Os eletrões de um ião podem encontrar-se em muitos níveis de energia (E1, E2, E3...).

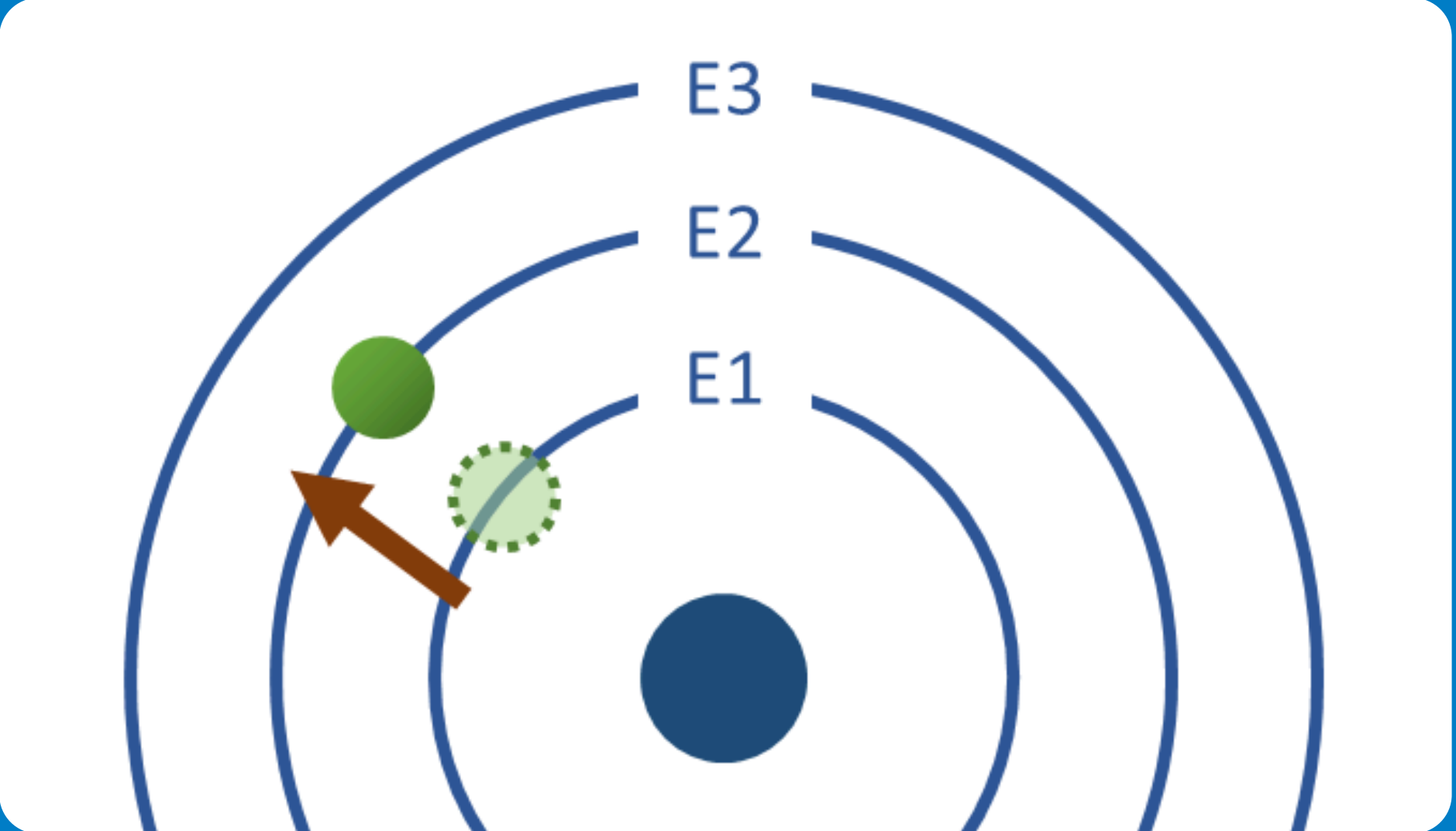


Tipicamente, utilizam-se dois estados (“0” e “1”), que resultam da estrutura eletrónica hiperfina. Esses dois estados formam o nosso *qubit*.

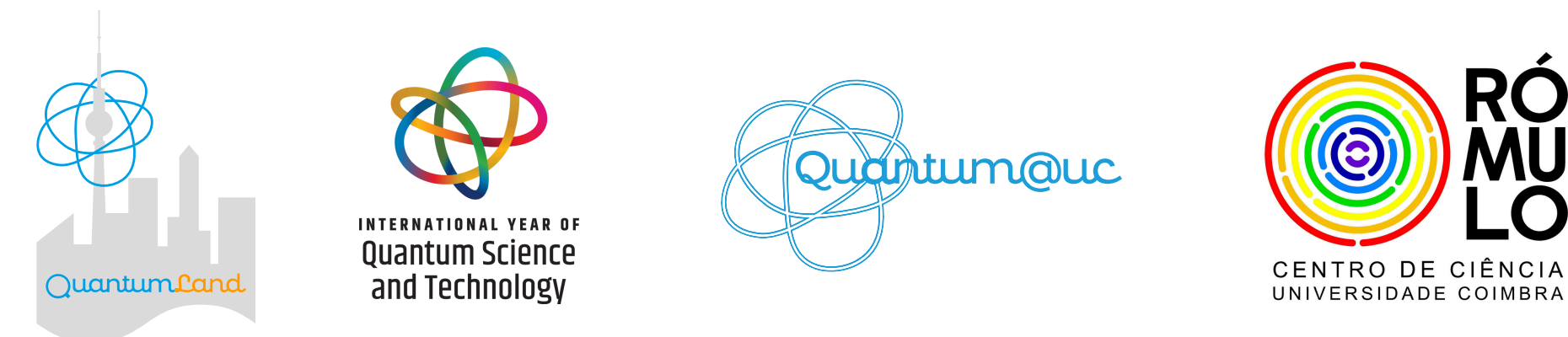
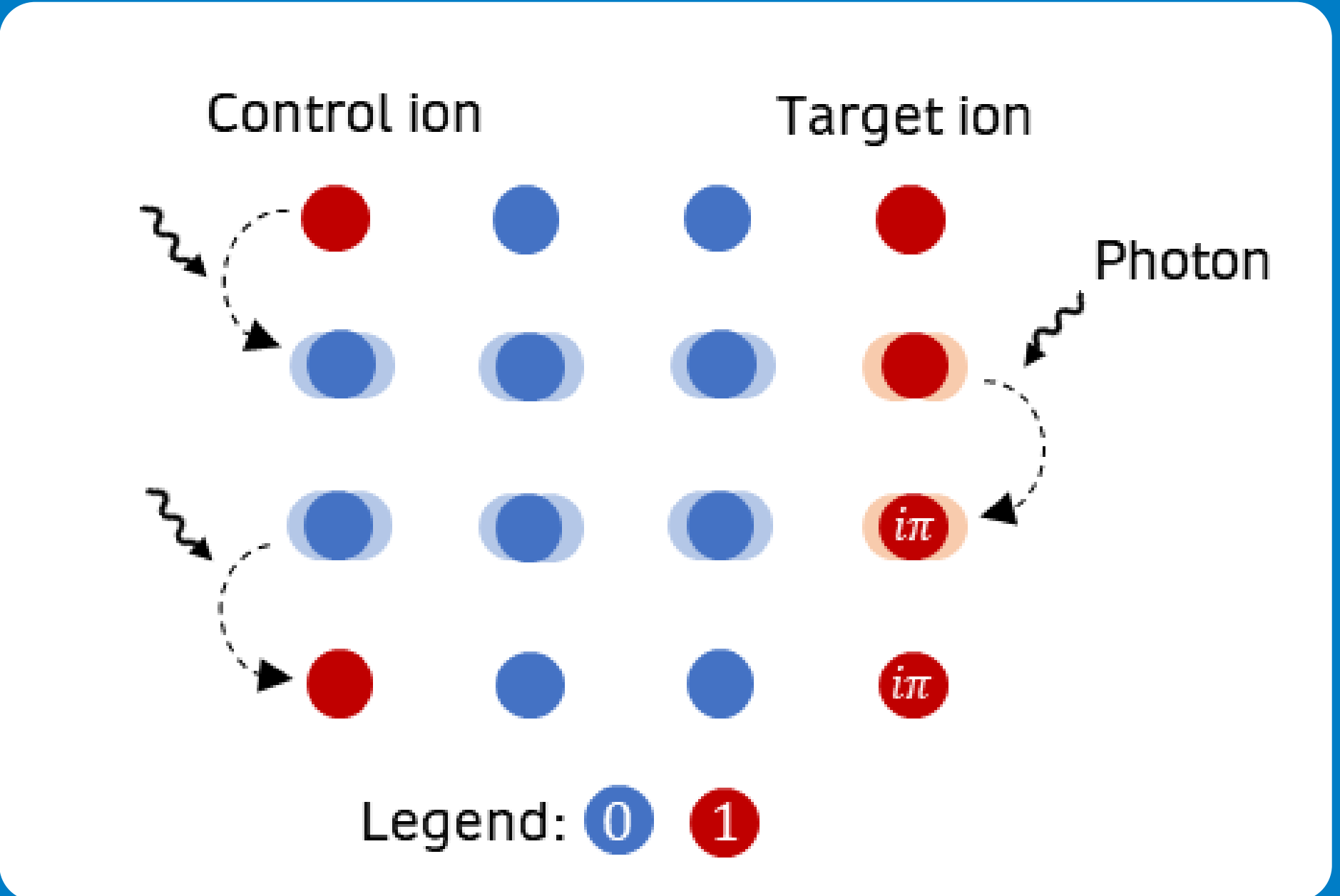
Estes estados têm um tempo de vida longo (*coerência*), pois são relativamente insensíveis a interações com o ambiente (sobretudo interações de dipolo elétrico), o que torna os decaimentos pouco prováveis.

Tecnologia para Computadores Quânticos

Operações de um qubit (como transitar de “0” a “1”) são induzidas por lasers ou microondas. Os eletrões interagem com os fótons externos e mudam de estado.



Operações de dois qubits utilizam o movimento coletivo dos iões como estados intermédios, que existem pela interação de Coulomb entre os iões. A operação de Cirac-Zoller (abaixo) foi a primeira a ser proposta.



Que mais é necessário para Computação Quântica?

De acordo com DiVincenzo, além de estados de qubit estáveis (*coerência*) e operações universais (*universalidade*), também é necessário conseguir *inicializar, medir e escalar* os computadores.

Desafios futuros

Atualmente, consegue-se *inicializar e medir qubits* com sucesso. O maior desafio para o futuro é conseguir *escalar* os computadores.

É preciso ter muitos qubits com qualidade para se implementar *correção de erros*. Isto é necessário para se conseguir implementar algoritmos úteis como o de Shor, que é capaz de fatorizar números em primos e tem implicações na criptografia.

ATOMIC QUANTUM COMPUTING WITH RYDBERG-INTERACTING QUBITS

Thomas Herrmann

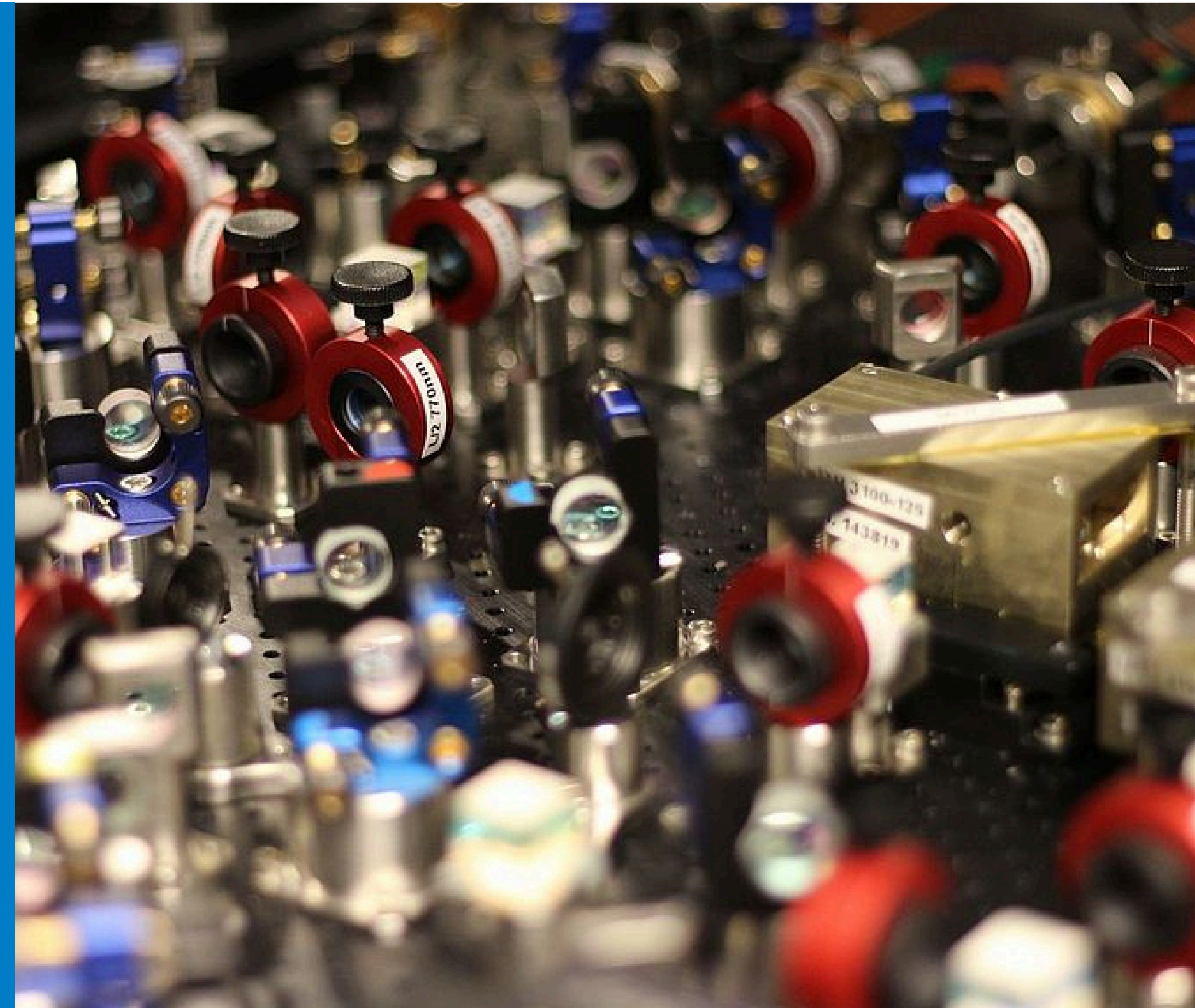
University of Coimbra

Technologies for Quantum Computers



Neutral Rydberg atoms (here strontium) in optical tweezers represent an alternative platform for QC.

A new possible way that could enable single qubit computations



This platform combines the indistinguishability of atomic qubits with precise control using laser light.

While aswell offering scalability in the size of the qubit register.

Single-qubit gates:

- Hadamard gates
- X, Y, Z gates

Multi-qubit gates:

- CNOT gate
- Controlled Z (CZ) gate

The logical states $|0\rangle$ and $|1\rangle$ are encoded into the zeeman sublevels of the ground state (S-orbital).

Raman oscillations between a P-orbital and the g.s. enable single qubit gates.

Combinations of target and control atoms and the Rydberg state enable multi qubit gates.

Single qubit gates:

By coupling the logical states $|0\rangle$ and $|1\rangle$, the system undergoes Rabi Oscillations. Precisely setting the Rabi frequency Ω applies different gate operations:

- X-Gate/bit flip (π -pulse)
- Hadamard-Gate ($\pi/2$ -pulse, creates superposition)
- Z-Gate/phase flip (applies phase shift)
- Y-Gate (combination of X and Z-Gate)

CZ-Gate:

Applies a phase shift of π to the $|11\rangle$ state, leaves other states unchanged.

$$|11\rangle \rightarrow -|11\rangle$$

CNOT-Gate:

Flips the target qubit, if the control qubit is in state $|1\rangle$, other states are unchanged.

$$|10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$

The Rydberg blockade allows controlled application of these operations

Combinations of single qubit and multi qubit gates enable Quantum computing.

Neutral rydberg atoms merge the perks of trapped ions and superconducting qubits, while offering a much greater qubit scale (up to 1000 qubits feasible)

DISTRIBUIÇÃO QUÂNTICA DE CHAVES: E91

Lara Antunes

Universidade de Coimbra

E91 é um **protocolo quântico de distribuição de chaves secretas** (Quantum Key Distribution, ou QKD) desenvolvido por Artur Ekert (1991). Este protocolo usa fótons entre a Alice e o Bob que, por estarem entrelaçados, permitem detetar interferências na comunicação. Assim, após garantir que não houve interceptação, a chave será utilizada para encriptar e decriptar mensagens entre a Alice e o Bob, garantindo comunicação segura.

Para formar a chave, o Charlie manda dois fótons entrelaçados (num estado de Bell) por um canal quântico – um para a Alice e outro para o Bob.

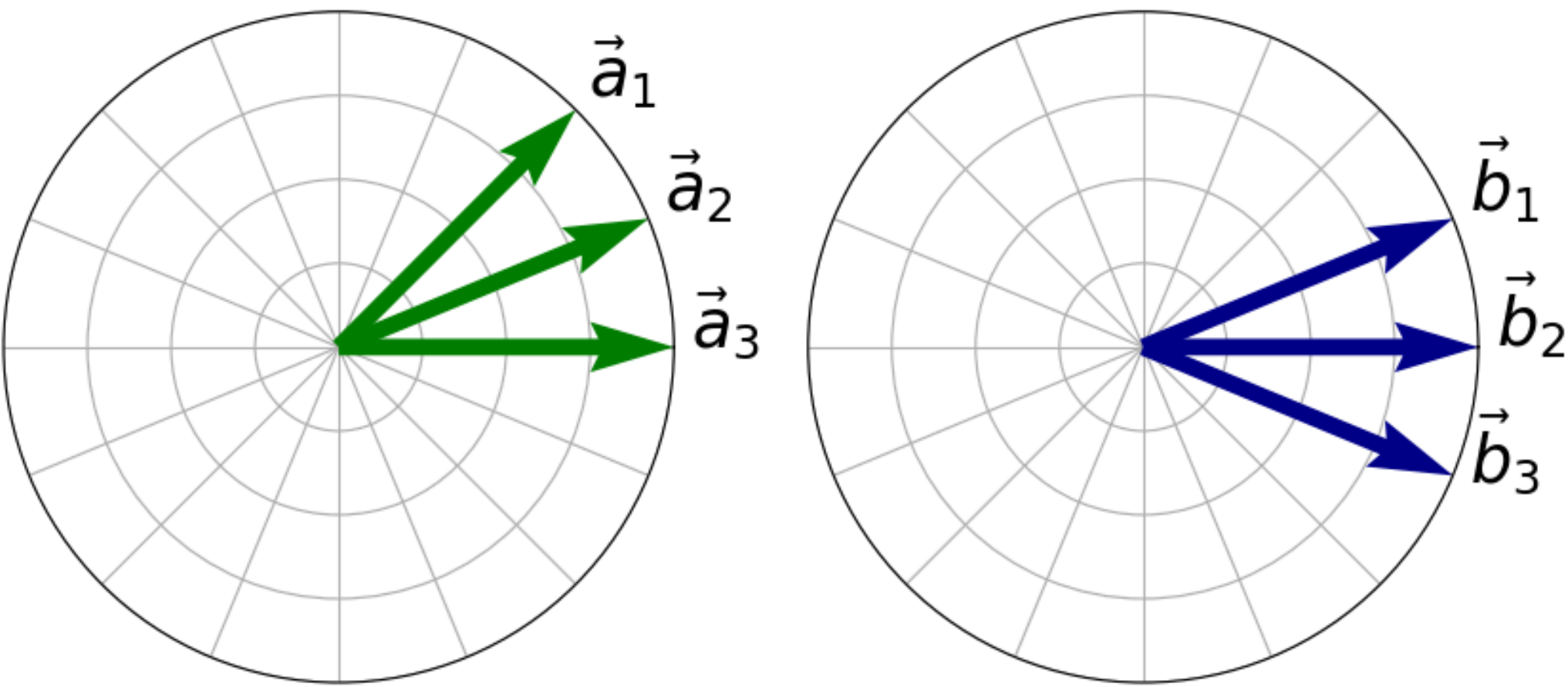
Os fótons estão num **estado de Bell**,

$$|\Phi^-\rangle = \frac{|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

Ao recebê-los, a Alice e o Bob escolherão uma base para medir a polarização do fóton. Ambos têm 3 bases entre as quais podem escolher.

Bases da Alice

Bases do Bob



Se as bases forem as mesmas, isto é, se forem

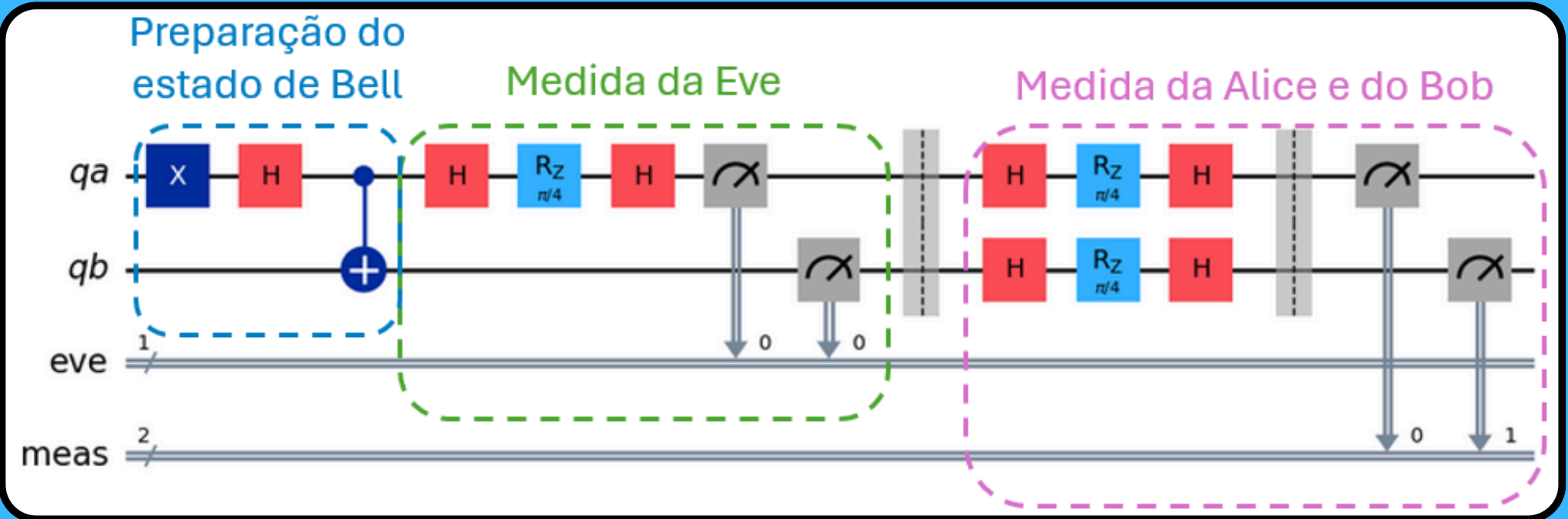
$$\left(\vec{a_2}, \vec{b_1}\right) \text{ ou } \left(\vec{a_3}, \vec{b_2}\right)$$

então ambos terão medido o qubit usando a mesma base. A medida levará à obtenção de um bit concordante com o estado de Bell inicial.

Sem interferência, as duas chaves serão iguais.

Comunicações Quânticas/Computação Quântica

Simulação com um Circuito Quântico



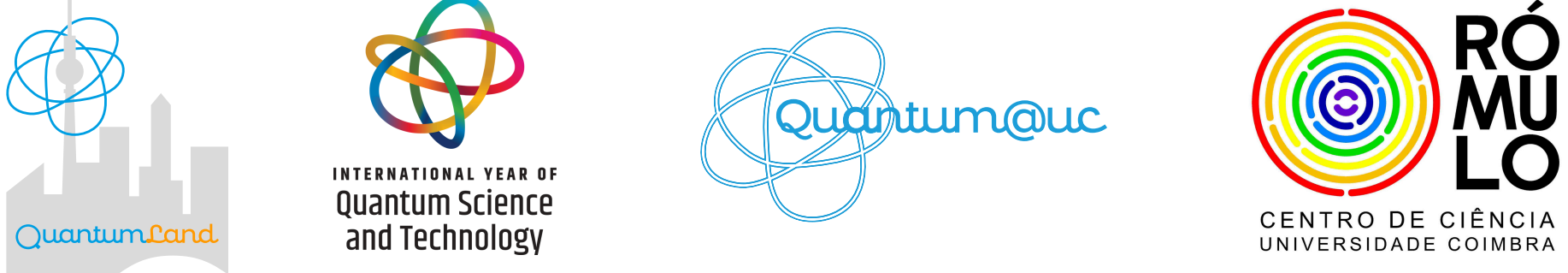
Resultados

Chave da Alice:
1011010101100010100010011
Chave do Bob:
101100001110010110010100

Observa-se que as chaves são diferentes, devido à interferência da Eve. No entanto, a Alice e o Bob não têm acesso à chave um do outro e irão realizar o teste de correlação para detetar a interceptação.

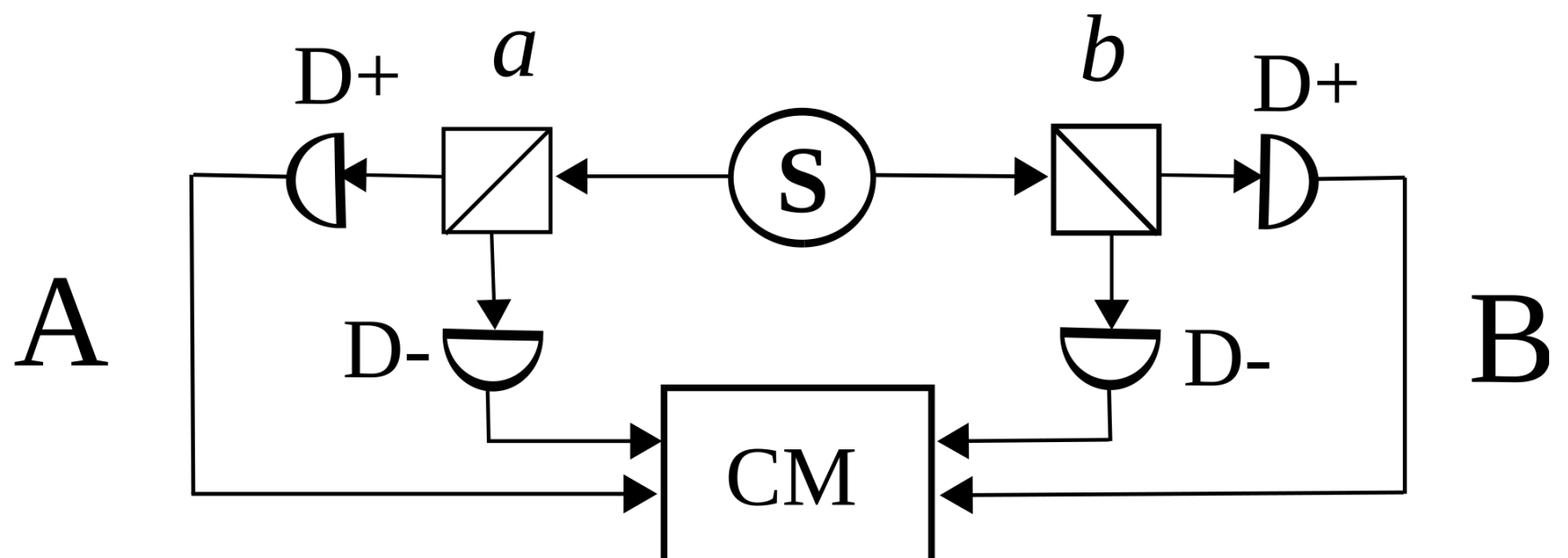
Eles irão partilhar as bases escolhidas um com o outro através de um canal clássico e formarão a chave com os bits das instâncias em que mediram com a mesma base.

A Alice e o Bob terão de realizar o teste de correlação CHSH, usando os bits que mediram em bases diferentes, para determinar se os fótons que receberam se encontravam entrelaçados, visto que, para os interceptar, a Eve tem de medir e reenviar os qubits. Deste modo, este teste deteta interferências com grande eficiência (para $S < 2$).



Teste de Bell

A fonte S (o “Charlie”) produz fótons entrelaçados e envia-os para os polarizadores, que podem ter direções $\alpha=0^\circ$ ou $\alpha'=45^\circ$ (no lado A) e $b=22.5^\circ$ ou $b'=-22.5^\circ$ (lado B). O sinal resultante é detetado e as contagens são registadas (++ , +- , -+ e --).



O valor de S é dado por

$$S = E(a, b) - E(a, b') + E(a', b) + E(a', b')$$

sabendo que, para cada par de orientações (a,b), o valor E é dado por

$$E(a, b) = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{++} + N_{+-} + N_{-+} + N_{--}}$$

CHSH correlation value

```
def test_correlation():
    a1b1 = [0,0,0,0]
    a1b3 = [0,0,0,0]
    a3b1 = [0,0,0,0]
    a3b3 = [0,0,0,0]
    for i in range(1000):
        if alicebase[i] == np.pi/2 and bobbase[i] == np.pi/4:
            if alicebits[i] == '0' and bobbits[i] == '0':
                a1b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '0':
                a1b3[i] += 1
            if alicebits[i] == '0' and bobbits[i] == '1':
                a3b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '1':
                a3b3[i] += 1
        if alicebase[i] == np.pi/2 and bobbase[i] == -np.pi/4:
            if alicebits[i] == '0' and bobbits[i] == '0':
                a1b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '0':
                a1b3[i] += 1
            if alicebits[i] == '0' and bobbits[i] == '1':
                a3b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '1':
                a3b3[i] += 1
        if alicebase[i] == -np.pi/2 and bobbase[i] == np.pi/4:
            if alicebits[i] == '0' and bobbits[i] == '0':
                a1b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '0':
                a1b3[i] += 1
            if alicebits[i] == '0' and bobbits[i] == '1':
                a3b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '1':
                a3b3[i] += 1
        if alicebase[i] == -np.pi/2 and bobbase[i] == -np.pi/4:
            if alicebits[i] == '0' and bobbits[i] == '0':
                a1b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '0':
                a1b3[i] += 1
            if alicebits[i] == '0' and bobbits[i] == '1':
                a3b1[i] += 1
            if alicebits[i] == '1' and bobbits[i] == '1':
                a3b3[i] += 1
    suma1b1 = sum(a1b1)
    suma1b3 = sum(a1b3)
    suma3b1 = sum(a3b1)
    suma3b3 = sum(a3b3)
    expa1b1 = (a1b1[0]-a1b1[1]-a1b1[2]+a1b1[3])/suma1b1
    expa1b3 = (a1b3[0]-a1b3[1]-a1b3[2]+a1b3[3])/suma1b3
    expa3b1 = (a3b1[0]-a3b1[1]-a3b1[2]+a3b1[3])/suma3b1
    expa3b3 = (a3b3[0]-a3b3[1]-a3b3[2]+a3b3[3])/suma3b3
    print(expa1b1)
    print(expa1b3)
    print(expa3b1)
    print(expa3b3)
    corr = expa1b1 - expa1b3 + expa3b1 + expa3b3
    print(corr)
```

Valor obtido: S = 1.7

S é menor que 2, logo a Alice e o Bob sabem com certeza que a sua comunicação foi interceptada.

Webgrafia
https://github.com/kardashin/E91_protocol/blob/master/E91_tutorial/E91_tutorial.ipynb
https://mpl.mpg.de/fileadmin/user_upload/Chekhov_a_Research_Group/Lecture_4_12.pdf
<https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.23.880>
https://en.wikipedia.org/wiki/Bell_test
<https://www.cleanpng.com/png-clip-art-scalable-vector-graphics-alice-and-bob-po-6428595/>

DISTRIBUIÇÃO QUÂNTICA DE CHAVES: SARG04

Diogo Ferreira

Universidade de Coimbra

O que é QKD?

A **distribuição quântica de chaves** (QKD) permite uma comunicação segura usando princípios da mecânica quântica para detetar qualquer tentativa de interceção.

Primeiro protocolo QKD

O primeiro protocolo QKD criado foi o **BB84**, desenvolvido por Charles Bennett e Gilles Brassard em 1984. O BB84 utiliza os estados de polarização dos fótons para codificar informação, permitindo a troca segura de chaves. A segurança reside na capacidade de detetar a presença de um intruso.

Porquê o SARG04?

As implementações práticas de QKD utilizam *lasers pulsados de baixa intensidade* como uma aproximação a fontes de fóton único. No entanto, esta escolha introduz vulnerabilidades, como os ataques de divisão do número de fótons (PNS), que exploram pulsos com múltiplos fótons para comprometer a segurança.

O SARG04 vem contrariar os ataques PNS alterando o **pós-processamento clássico** do BB84, ou seja, a informação clássica transmitida pela Alice e depois pelo Bob.

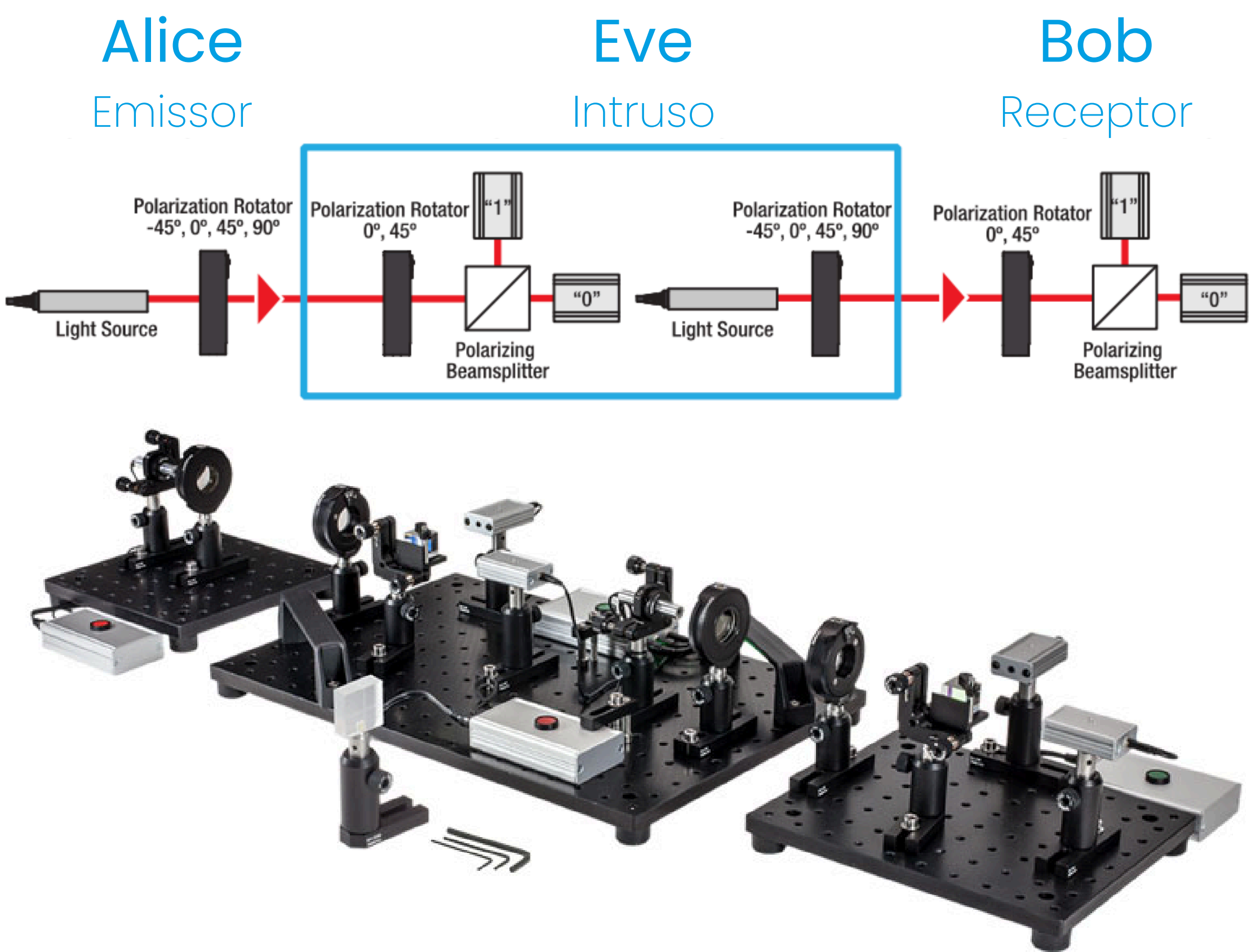
Qubits

Um qubit (bit quântico) é a unidade fundamental de informação na computação quântica, podendo existir em **sobreposição** de estados $|0\rangle$ e $|1\rangle$ simultaneamente. Tanto pode ser um fóton com várias polarizações, bem como um átomo com um spin $\uparrow$ ou $\downarrow$. Os estados $|+\rangle$ e $|-\rangle$ são exemplos de uma sobreposição em que há 50% de probabilidade de se medir “0” ou “1”.

Ataques PNS

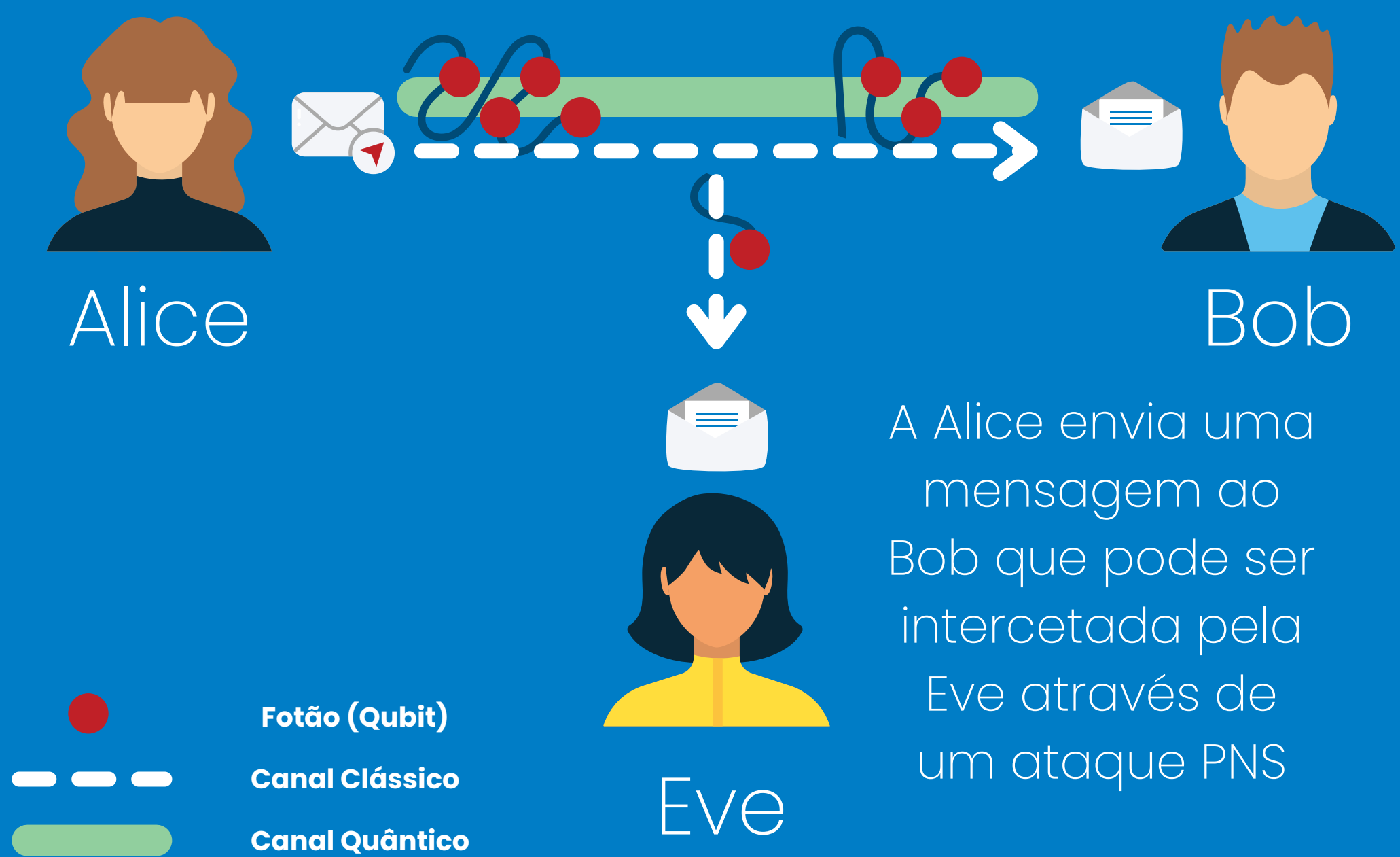
Os **ataques Photon Number Splitting (PNS)** exploram a vulnerabilidade dos *lasers pulsados de baixa intensidade*. O número de fótons por pulso segue uma distribuição de Poisson e é inevitável haver alguns pulsos com mais do que um fóton, criando uma repetição indesejada de informação.

Kit de demonstração BB84

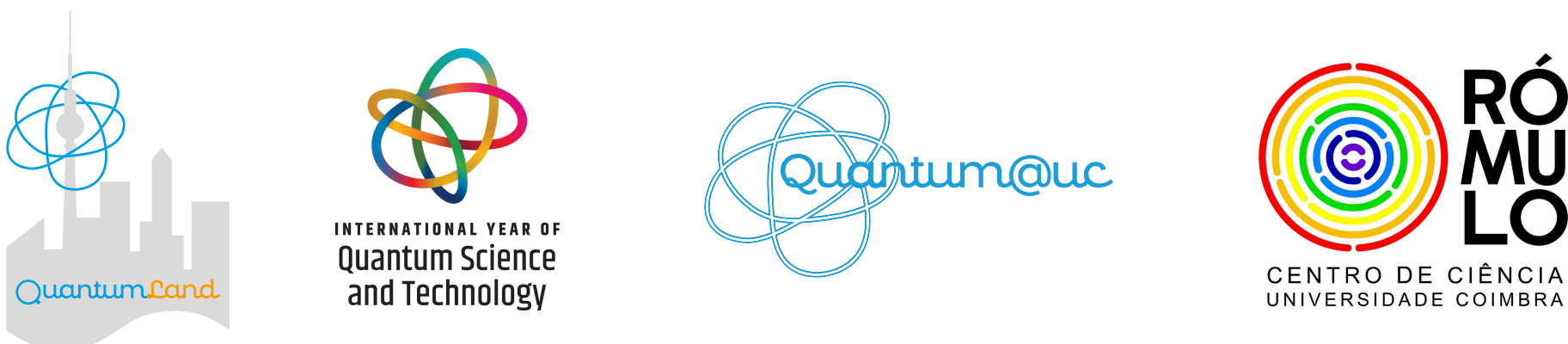


Comunicações quânticas/Computação quântica

Protocolo SARG04



1. A **Alice gera** duas matrizes aleatórias de números binários: os **Bits** de informação e as **Bases** de codificação. Conforme o bit e a base escolhidos, a alice **codifica** o qubit em 4 estados possíveis $|0\rangle, |1\rangle, |+\rangle$ e $|-\rangle$.
2. A Alice envia a mensagem ao Bob.
3. O **Bob gera** uma matriz aleatória de números binários que será a sua **Base** de decodificação e **lê** a mensagem com ela **obtendo** uma matriz de **Bits**.
4. A **Alice envia** ao Bob **um par dos 4** estados iniciais, de bases diferentes, onde **somente 1** dos estados é o **correto**, isto para cada qubit. Conforme o bit obtido e a base escolhida pelo **Bob**, o mesmo **avalia** se consegue saber com certeza qual dos 2 estados é o **correto**. Conforme a sua decisão **informa a Alice** se o descartou ou não.
5. Correção de erros e amplificação de privacidade.



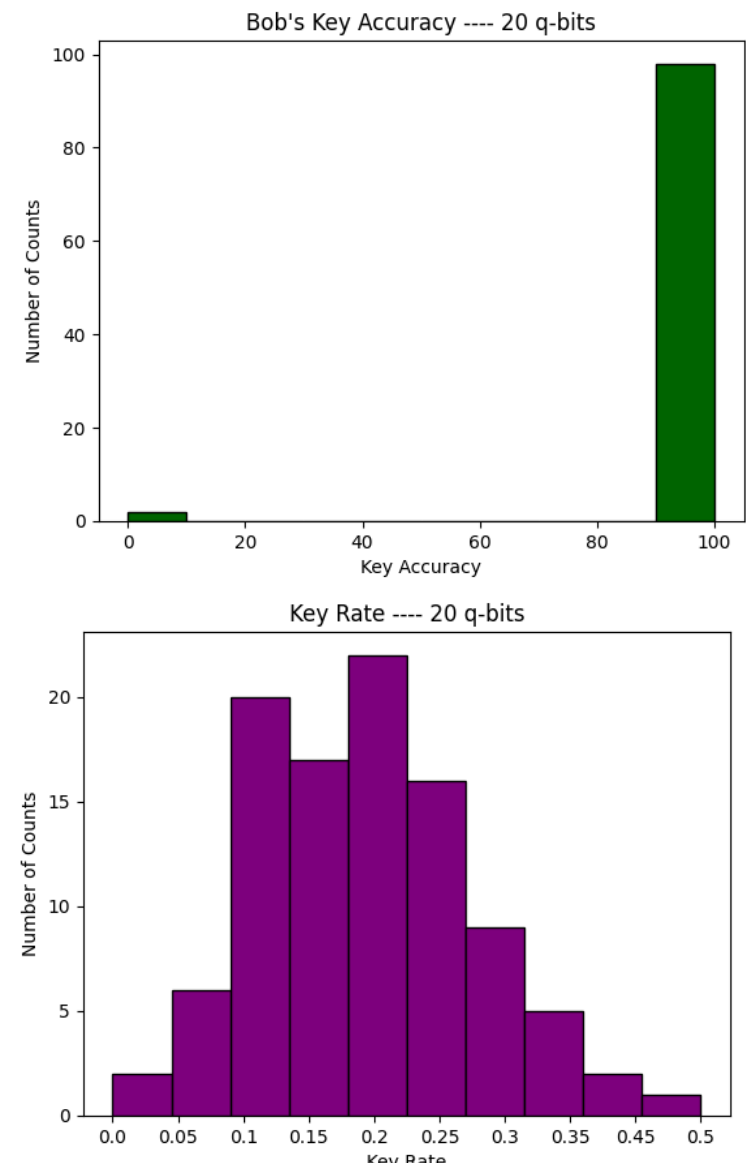
Simulação em qiskit

Para verificar a taxa de qubits validados (**Key Rate**) e a taxa de erro comparando a chave do Bob com a da Alice (**Key Accuracy**), foi simulado o protocolo no IBM Qiskit, usando o simulador Aer.

Resultados

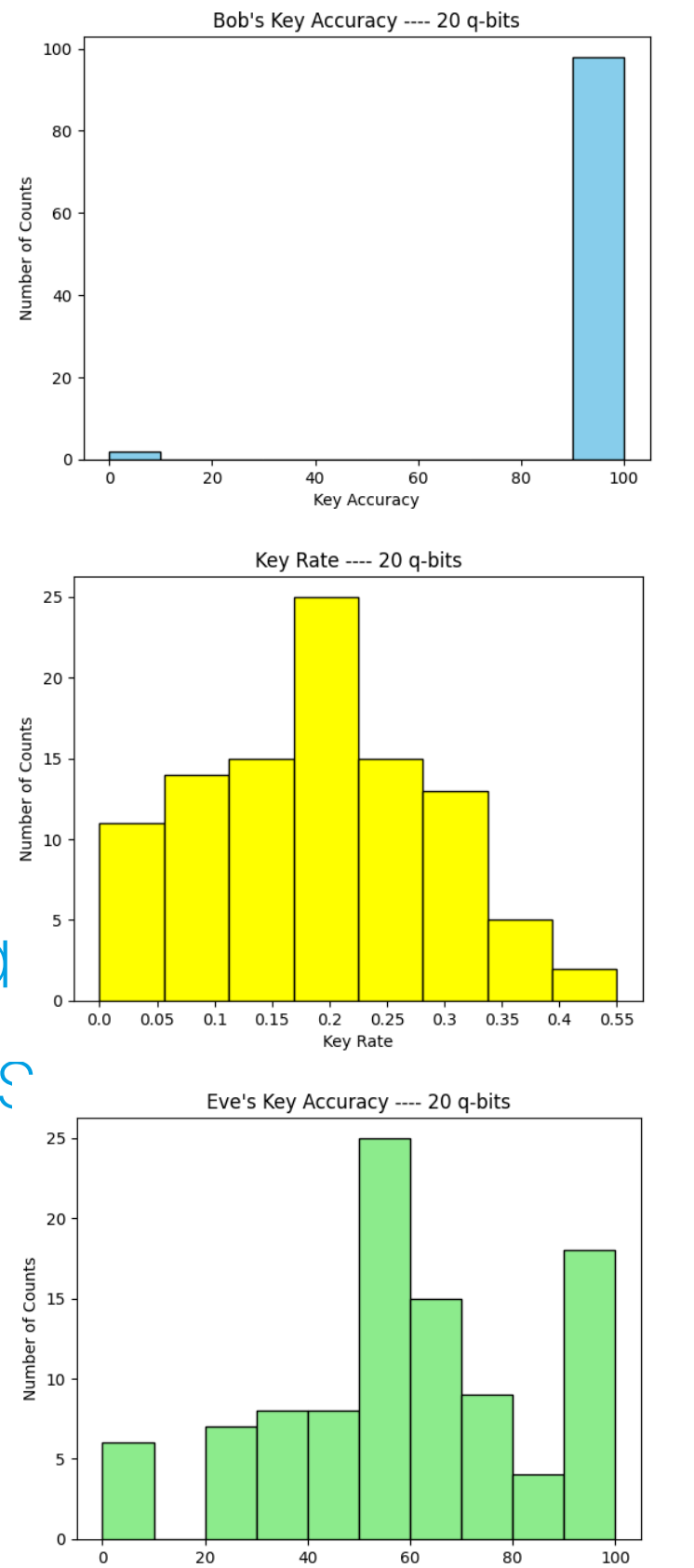
Alice -----> Bob

Podemos verificar que em quase todos os casos a chave do Bob correspondeu à da Alice.



Alice ---> Eve ---> Bob

Mesmo com a intrusão da Eve é possível observar que a compatibilidade de chaves entre o Bob e a Alice se mantém, mas a da Eve com a Alice é má, tal como esperado. Somente é boa para chaves pequenas onde a probabilidade das chaves diferirem é muito baixa.



Conclusões

Como podemos observar o SARG04 é **bastante fiável** na transmissão de informação, tal como na proteção dessa informação tendo uma média de taxas de **qubits validados** igual a **1/4** dos qubits, corroborando a teoria presente na literatura.

DISTRIBUIÇÃO QUÂNTICA DE CHAVES:

BB84 E B92

Maria Luísa Mendes
Universidade de Coimbra

A **distribuição quântica de chaves** (QKD) é um método de comunicação que garante trocas seguras de chaves de encriptação entre utilizadores.

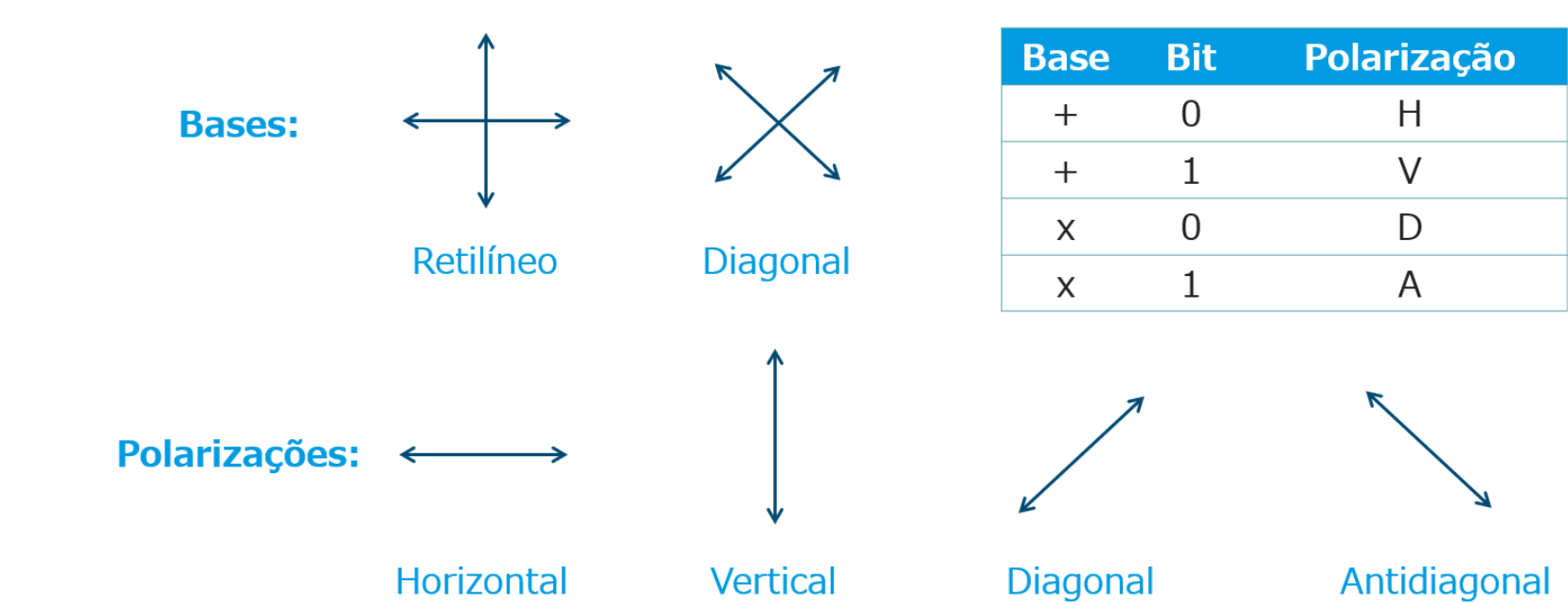
Este método utiliza a física quântica para trocar chaves criptográficas de uma forma que pode detetar a interferência de intrusos

O Protocolo B92

Este protocolo foi introduzido em 1992 por Charles Bennett. Trata-se de uma versão modificada do BB84, utilizando apenas 2 estados de polarização diferentes, um da base diagonal e outro da base rectilínea. Além disso, durante a criação da chave, o Bob não precisa de anunciar a sua escolha de base, apenas partilha certos resultados das suas medições. Se o bit medido não estiver de acordo com o resultado específico, é descartado, formando-se assim uma chave.

O Protocolo BB84

Foi introduzido em 1984 por Charles Bennett e Gilles Brassard. É caracterizado pela existência de um canal quântico e de um canal clássico que podem ser utilizados simultaneamente para partilhar informações sobre chaves criptográficas.



Os fótons enviados através da interação são polarizados de acordo com a base diagonal (X) e a base rectilínea (+). O BB84 utiliza quatro estados de polarização diferentes, dois de cada base, cada um correspondendo aos números binários 1 ou 0.

Formação da Chave

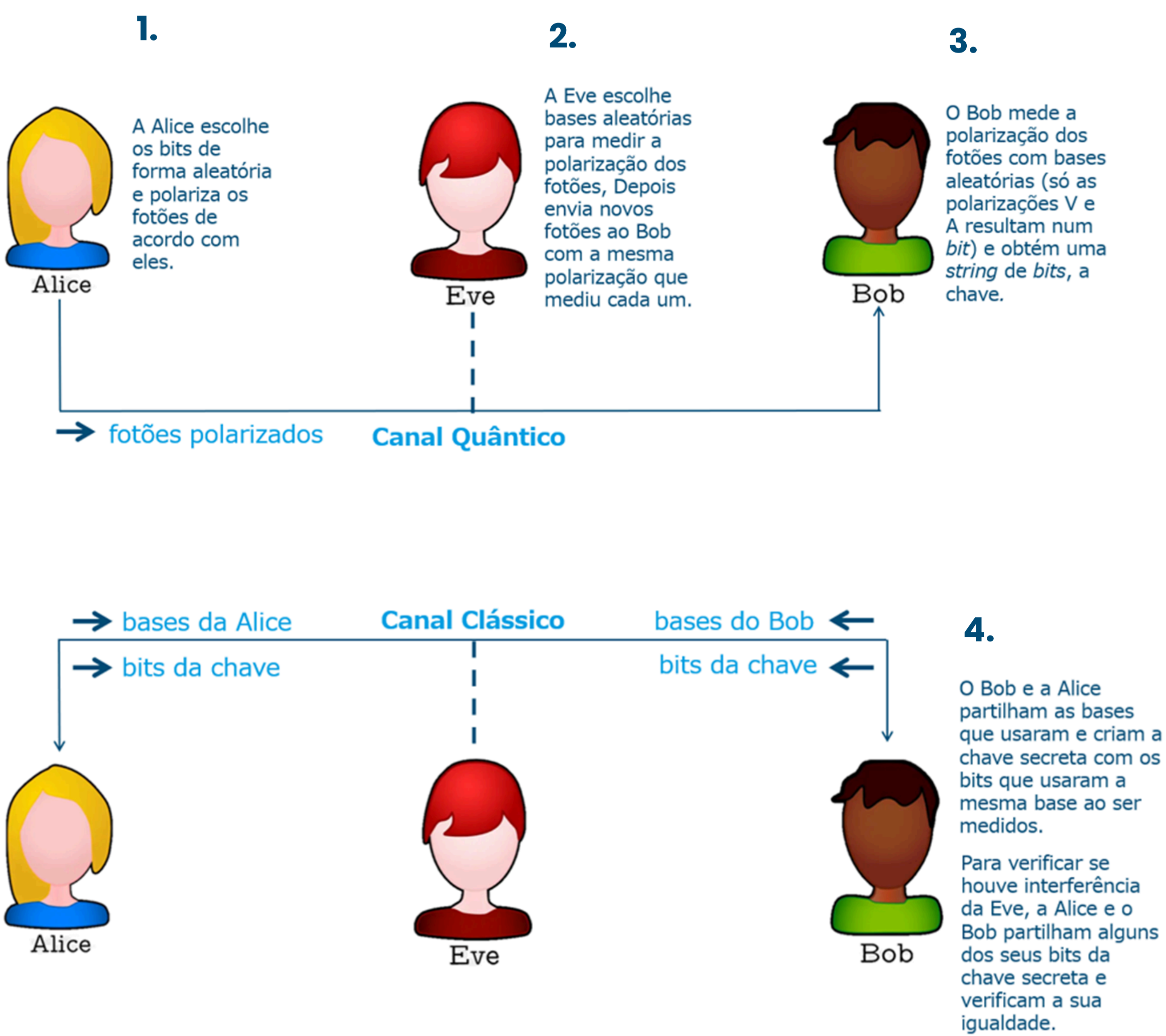
Se o Bob seleccionar a mesma base que a Alice para o mesmo qubit, obtém o bit pretendido enviado pela Alice. Se o Bob usar uma base diferente durante a medição, obterá um bit aleatório. A chave só é formada depois de Alice e Bob comunicarem e compararem a base utilizada para cada qubit. No protocolo BB8,4 se a base utilizada for igual entre os dois, adiciona-se o bit à chave. Sem Interferências, a Alice e o Bob têm uma chave idêntica.

BB84	Sequência de bits da Alice	0	1	1	0	0	0	0	1	1	1
	Bases da Alice	+	+	X	+	+	+	+	+	+	+
	Bases do Bob	+	X	X	X	X	X	+	+	+	X
	Sequência de bits do Bob	1	1	1	1	0	1	1	1	1	0
	Chave Bob	1	-	1	-	-	-	1	1	1	-
	Chave Alice	0	-	1	-	-	-	0	1	1	-

B92	Sequência de bits da Alice	H	D	H	D	H	H	H	D	D	D
	Bases do Bob	+	+	X	+	X	X	X	+	X	X
	Sequência de bits do Bob	H	A	V	H	V	V	D	H	D	D
	Chave Bob	-	1	0	-	0	0	-	-	-	-
	Chave Alice	-	1	0	-	0	0	-	-	-	-

Comunicações Quânticas/Computação Quântica

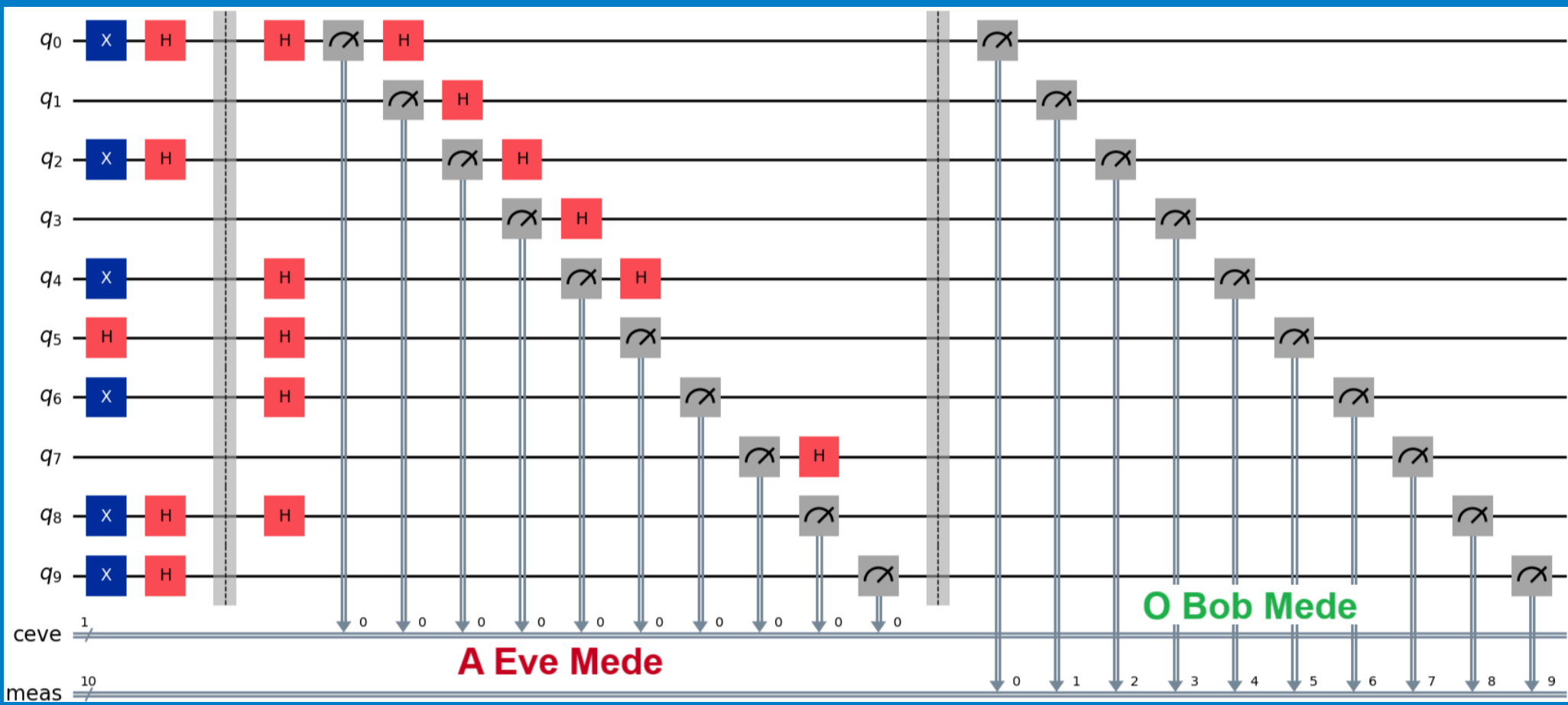
- Alice envia os fótons polarizados ao Bob através do canal quântico. Por exemplo,
Lista de bits da mensagem: [0,1,1,0,0,0,0,1,1,1]
Lista das bases da Alice: [0,0,1,0,0,0,0,0,0,0]
- A Eve pode interceptar a mensagem (ela mede numa base aleatória). Depois, envia os seus resultados ao Bob, em bits polarizados de acordo com as bases que escolheu.
- Bob recebe e mede os qubits usando uma base aleatória para cada, obtendo uma sequência de bits. Por exemplo,
Lista das bases do Bob: [0,1,1,1,1,1,0,0,0,1]
Sequência do Bob: [1,1,1,1,0,1,1,1,1,0]
- Alice e Bob partilham as suas bases através do canal clássico e formam a chave.



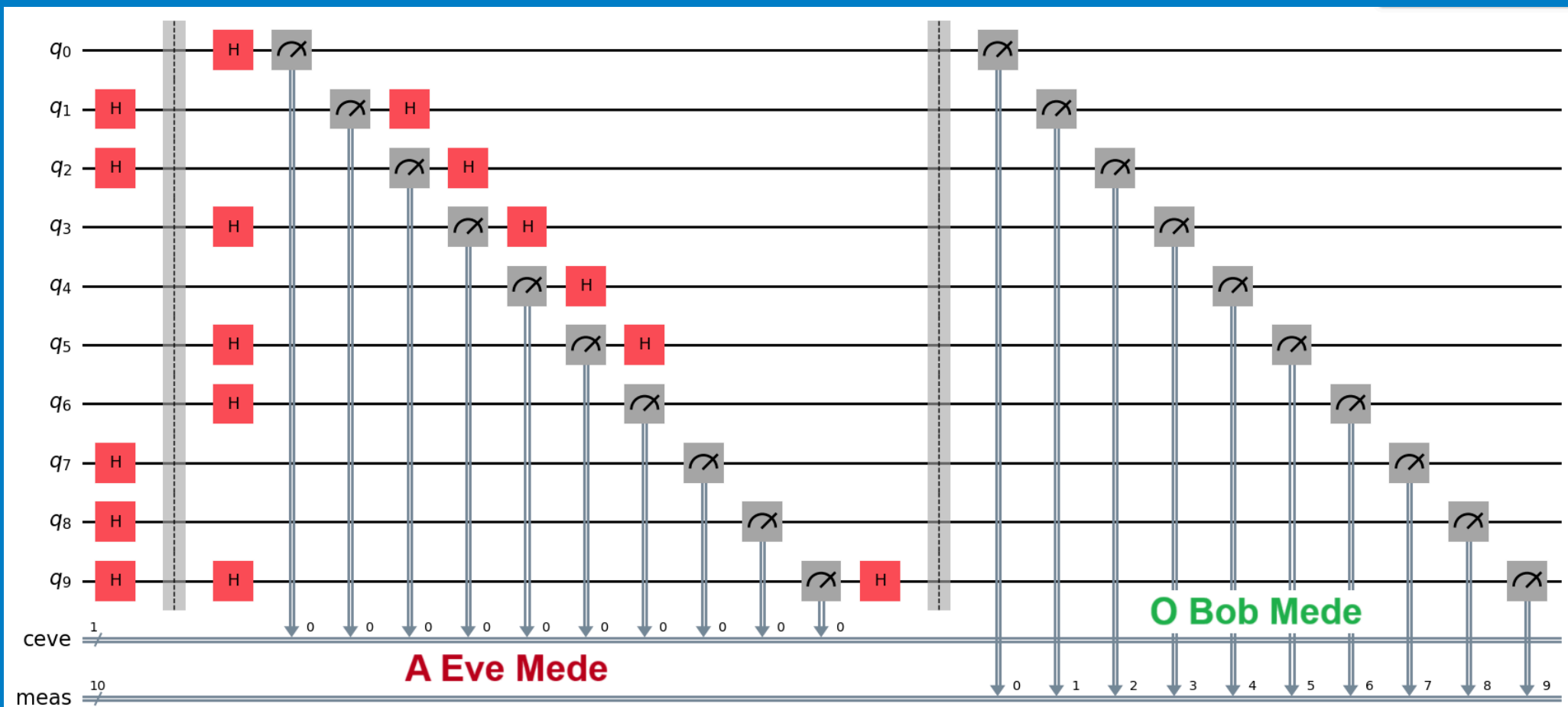
As interferências de intrusos (Eve) resultam em “erros” nas chaves de encriptação. Para detetar a presença de erros/intrusos, a Alice e o Bob devem partilhar entre si partes da chave criada. Se houver inconsistências a chave é descartada e o protocolo é repetido.

A presença da “Eve” traduz-se numa taxa de erro de 18.7% num sistema ideal no qual a Eve é a única fonte de erro

Simulação em Qiskit BB84



B92

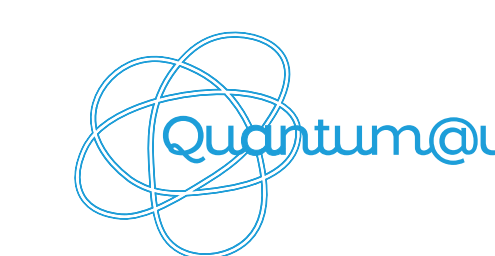


GERADOR QUÂNTICO DE NÚMEROS ALEATÓRIOS (QRNG)

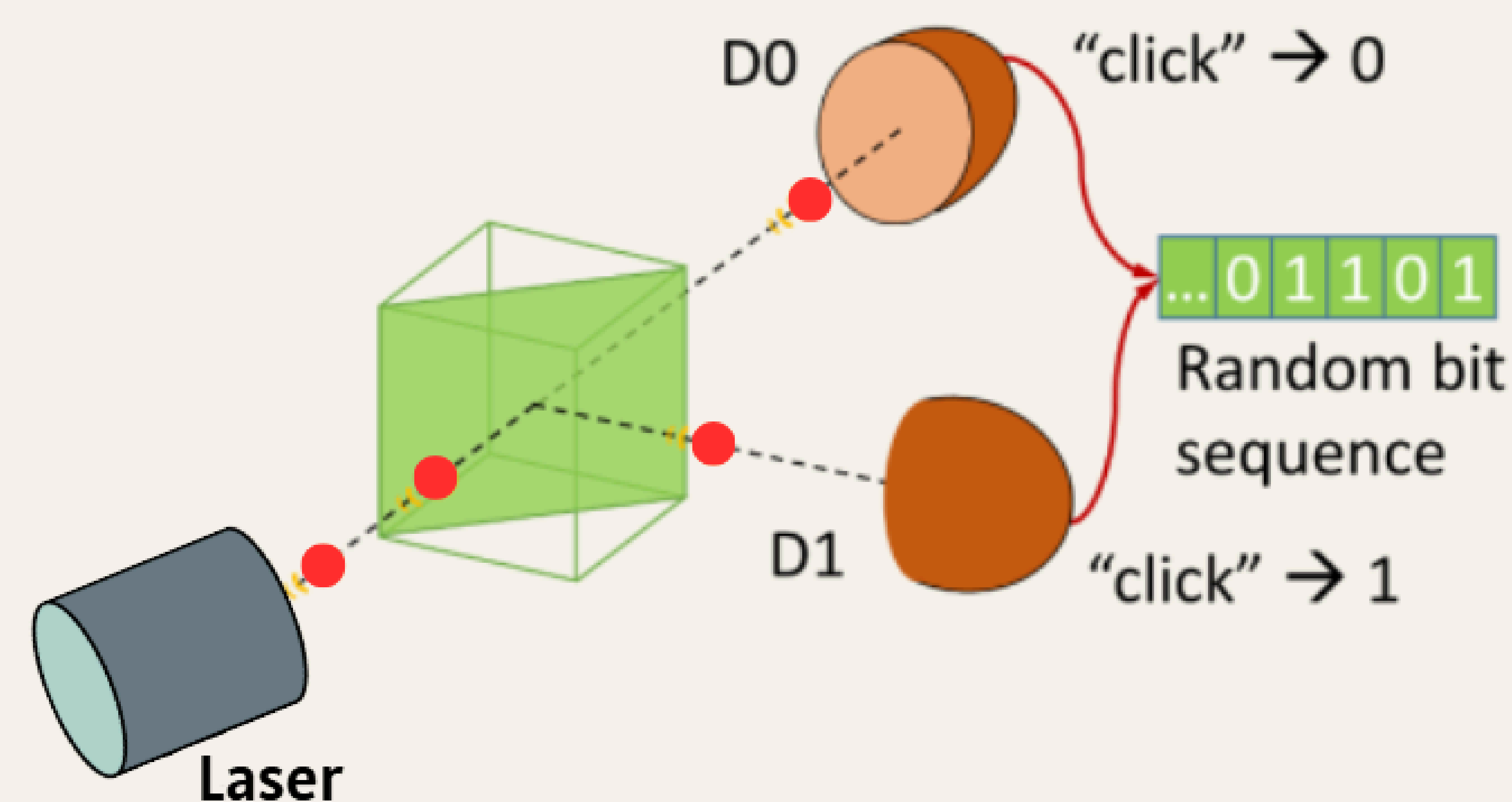
Bárbara Baptista

Universidade de Coimbra

Tecnologias Quânticas



Os **QRNGs** utilizam princípios da mecânica quântica para gerar uma sequência de números verdadeiramente aleatórios. Eles exemplificam uma aplicação prática dos princípios da Mecânica Quântica, nomeadamente a aleatoriedade associada à medida de um estado quântico.



Existem três tipos de RNGs: Quantum RNGs, True RNGs e Pseudo-RNGs. Os QRNGs são os mais seguros e imprevisíveis, mas também os mais caros. Os Pseudo-RNGs são os mais acessíveis, mas comprometem a segurança e qualidade da aleatoriedade. Já os TRNGs oferecem um equilíbrio entre os dois.

Princípio de funcionamento

No exemplo da figura, um laser emite fótons individuais, polarizados, que são uma sobreposição de um estado com polarização vertical e outro com polarização horizontal. Os fótons incidem num divisor de feixe que funciona como uma medida do estado de polarização do fóton.

O fóton pode sair do divisor de feixe com polarização vertical, em direção ao detetor D0, ou sair com polarização horizontal, em direção a D1. Os detetores contam fótons. Um *click* em D0 é um 0, um *click* em D1 é um 1. A sequência de *clicks* é uma sequência aleatória de bits. **A aleatoriedade é garantida pela imprevisibilidade da medida em Mecânica Quântica.**

Aplicações:

- Geração de chaves quânticas para segurança digital.
- Simulações em modelos complexos.
- Gaming e tecnologia IoT

Perspetivas futuras

No presente, os QRNGs já são utilizados em sistemas de distribuição de chaves quânticas.

Com o desenvolvimento das tecnologias quânticas espera-se que os QRNGs venham a desempenhar um papel importante em computação quântica e na segurança digital.

ENTANGLEMENT SWAPPING

André Roque

Universidade de Coimbra

Entanglement swapping é um processo para entrelaçar duas partículas, sem que estas tenham interagido anteriormente.

É um fenómeno quântico explorado e utilizado atualmente, sendo uma das peças fulcrais para o desenvolvimento de sistemas de comunicação quânticos.

Demonstração

Este fenómeno foi demonstrado pela primeira vez experimentalmente em 1998, por Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, e Anton Zeilinger.

Como funciona?

Para entrelaçar as partículas 1 e 4, sem elas interagirem entre si, entrelaçamo-las com duas novas partículas, 2 e 3.

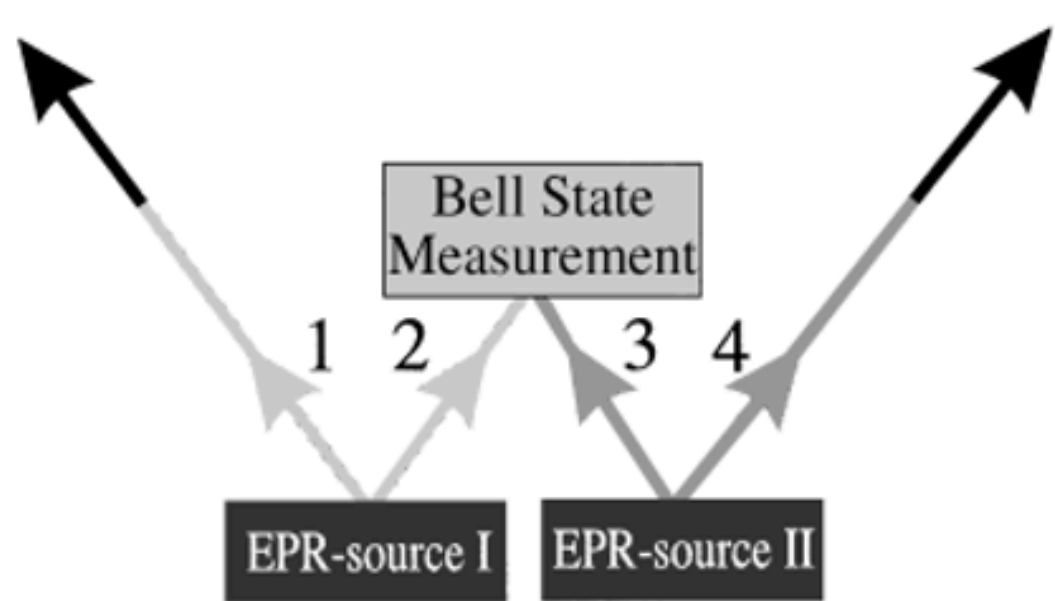


Preparamos os pares (1, 2), (3,4) em estados de Bell (ou pares EPR):

$$|\Psi\rangle_{1234} = \frac{1}{2}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2) \otimes (|H\rangle_3|V\rangle_4 - |V\rangle_3|H\rangle_4)$$

Tecnologias Quânticas

Medindo 2 e 3 na base de Bell,



estas são projetadas sobre um dos 4 estados de Bell,

$$|\Psi^\pm\rangle_{23} = \frac{1}{\sqrt{2}}(|H\rangle_2|V\rangle_3 \pm |V\rangle_2|H\rangle_3)$$
$$|\Phi^\pm\rangle_{23} = \frac{1}{\sqrt{2}}(|H\rangle_2|H\rangle_3 \pm |V\rangle_2|V\rangle_3)$$

ficando estas, assim como o par que não interagiu, entrelaçadas.



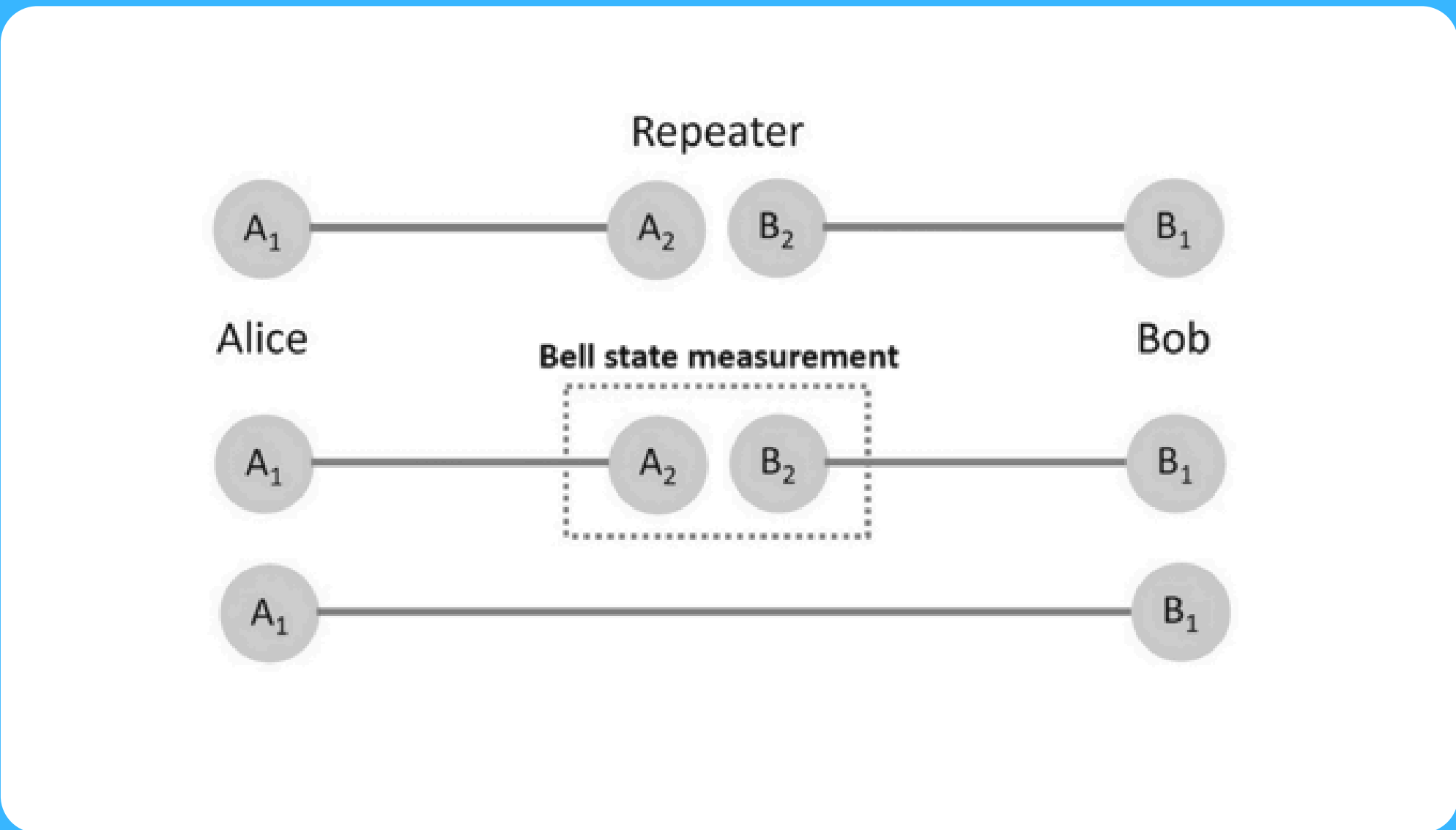
Cubesat alemão QUBE, lançado em agosto de 2024, no âmbito de teste de QKD.

Aplicação: Quantum networks

As **redes quânticas** unem vários processadores quânticos, que partilham informação na forma de qubits através de canais quânticos, por exemplo, fótons polarizados, enviados pelos canais de fibra ótica já existentes.

Ao percorrer longas distâncias, a coerência do sinal é perdida. É necessária a utilização de um repetidor de sinal não clássico.

Os **repetidores quânticos** utilizam entanglement swapping como princípio essencial. Reduzem a metade o caminho que o sinal precisa viajar.



Na atualidade

- O satélite chinês Micius (2016), realiza 4 experiências no âmbito de QKD, entanglement swapping e comunicações quânticas.
- O cubesat alemão QUBE (agosto de 2024), visa testar processos de QKD
- O satélite europeu EAGLE-1, previsto para finais de 2025, testará QKD em quantum networks com satélites, estando o projeto EAGLE-2 em desenvolvimento.

RELÓGIOS ATÔMICOS

Marcela Arostegui

Universidade de Coimbra

O que são?

Relógios atômicos medem o tempo ajustando e mantendo a frequência de um oscilador macroscópico, usando como referência a frequência de uma transição atômica .

Como funcionam?

1 Estrutura hiperfina

Usam a frequência de oscilação precisa de transições hiperfinas dos átomos como referência

2 Sintonização de micro-ondas/laser

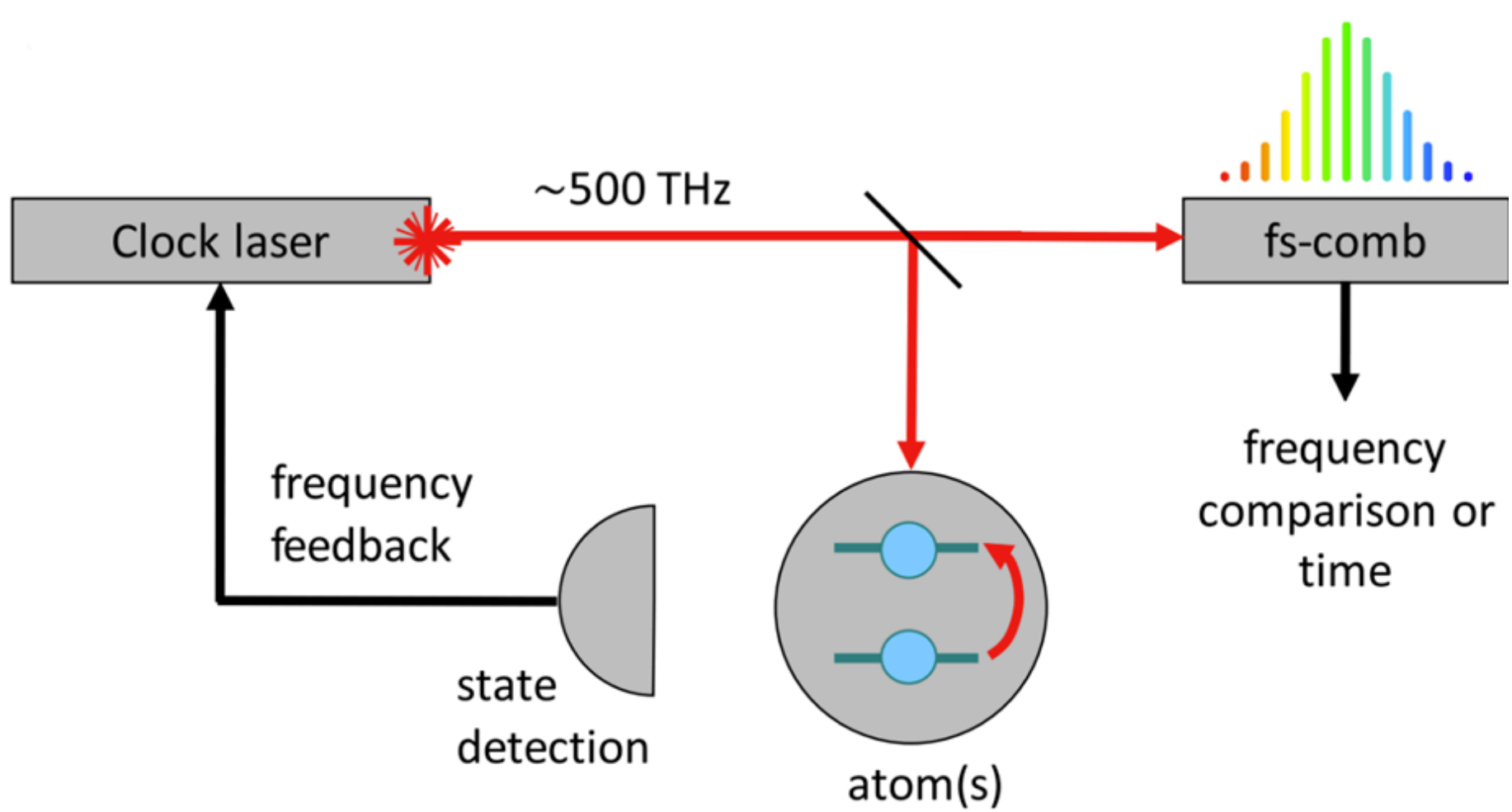
Ondas geradas por lasers ou microondas são escolhidas para coincidir com a frequência da transição, mantendo os átomos em oscilação

3 Loop de Realimentação

Parte do sinal é realimentado para ajustar o laser à frequência real

4 Medição dos ciclos

O tempo é medido de acordo com a quantidade de ciclos

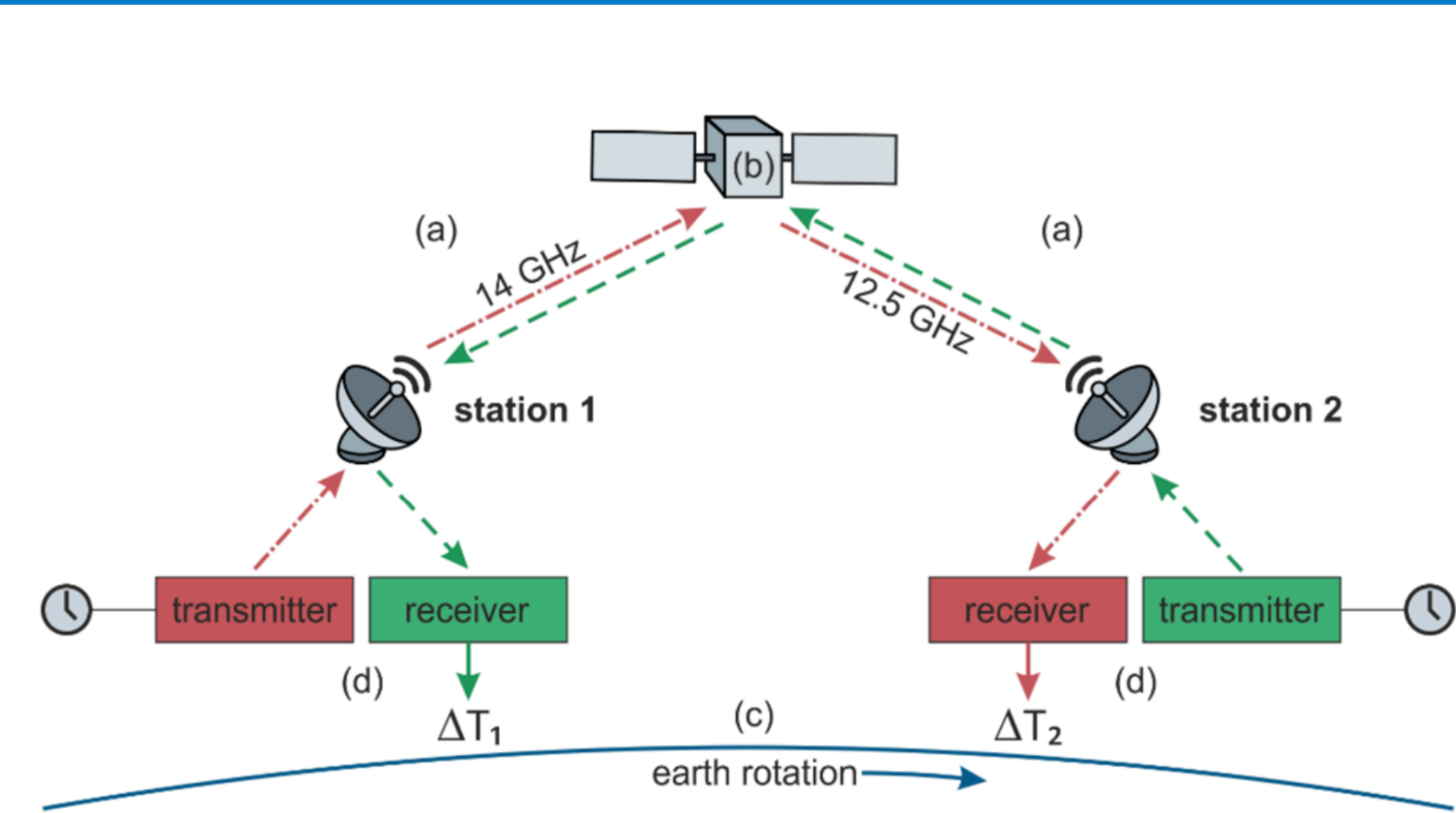


Aplicações

Física Fundamental: usados em estudos como detecção de matéria escura, ondas gravíticas e relação entre a quântica e a relatividade geral

Navegação e Comunicação no Deep Space: A cronometragem precisa permite a navegação e o envio/receção de informações de naves espaciais em missões interplanetárias

Exemplo: Sinais GPS e GNSS
Ao comparar tempos de vários satélites com relógios atômicos, calcula-se a posição com elevada precisão, corrigindo efeitos relativísticos



Tecnologias Quânticas

O Futuro dos Relógios Atômicos

Relógios Atômicos Óticos

Usam átomos arrefecidos a laser (~10¹⁴ Hz), alcançando maior precisão do que os relógios de micro-ondas (~10⁹ Hz)

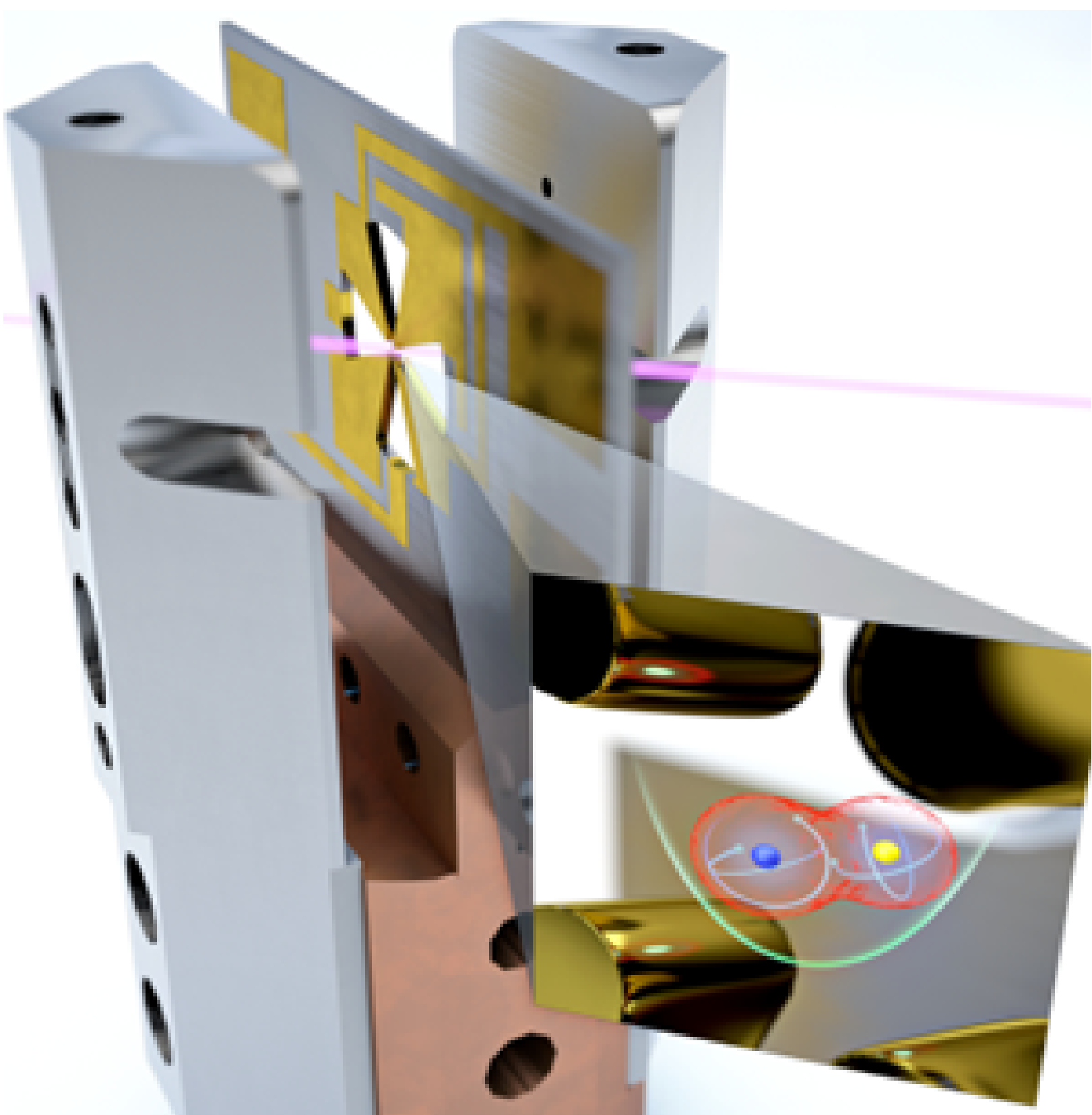
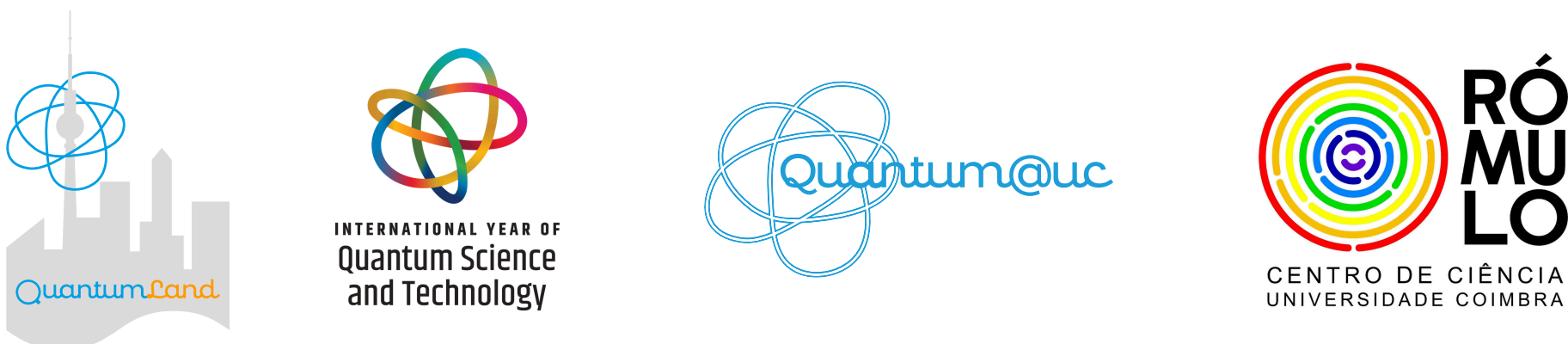
Relógios de Átomos Frios:

Baixam a temperatura dos átomos até valores próximos do zero absoluto, reduzindo o movimento térmico, o que aumenta a estabilidade

Relógios com *ion traps*: Isolam iões individuais em *ion traps* eletromagnéticas, minimizando a interferência externa, o que aumenta a precisão

Relógios de Lógica Quântica

Usam entrelaçamento quântico e manipulação de estados quânticos em *ion traps* (estrutura dourado com recorte em forma de cruz na figura em cima) para aumentar a precisão.



Perspetivas futuras

Os relógios atômicos são fundamentais em navegação, no GPS, na cronometragem global e nas telecomunicações.

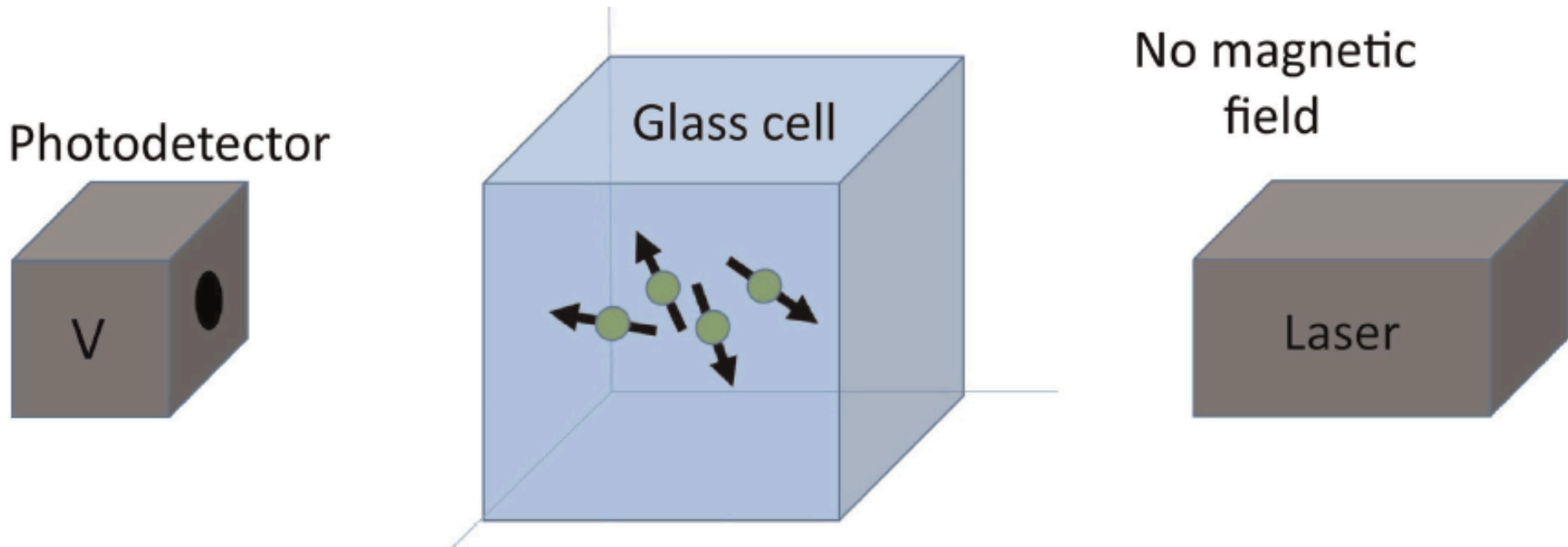
Continuam a ser desenvolvidos novos tipos de relógios atômicos, procurando aumentar a sua precisão e estabilidade. A tecnologia associada a computadores quânticos cria novos caminhos a explorar.

OPTICALLY PUMPED MAGNETOMETERS (OPMs)

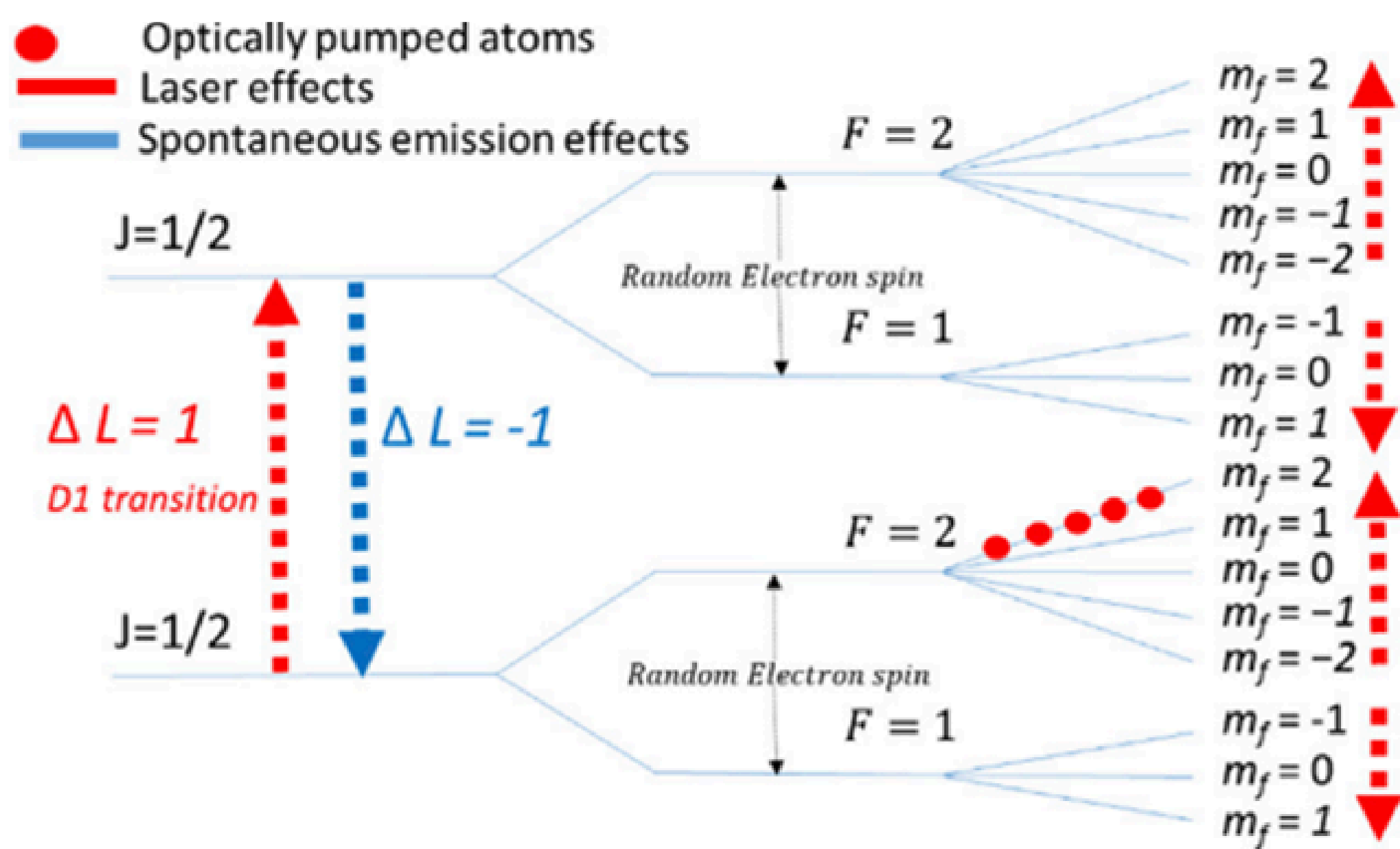
Patrícia Bartolomeu

Universidade de Coimbra

OPMs são sensores quânticos de campo magnético constituídos por um sistema de estimulação ótica (laser), uma célula de vapor com átomos alcalinos (como o Rubídio) e um fotodetetor.



O funcionamento destes sensores baseia-se na manipulação do spin atómico através da ação de luz laser. Usando luz circularmente polarizada e um campo aplicado muito baixo, os átomos adquirem uma polarização de spin e deixam de absorver radiação. Na presença do campo externo que se pretende medir, o spin precisa na direção do campo e a intensidade da luz transmitida diminui.

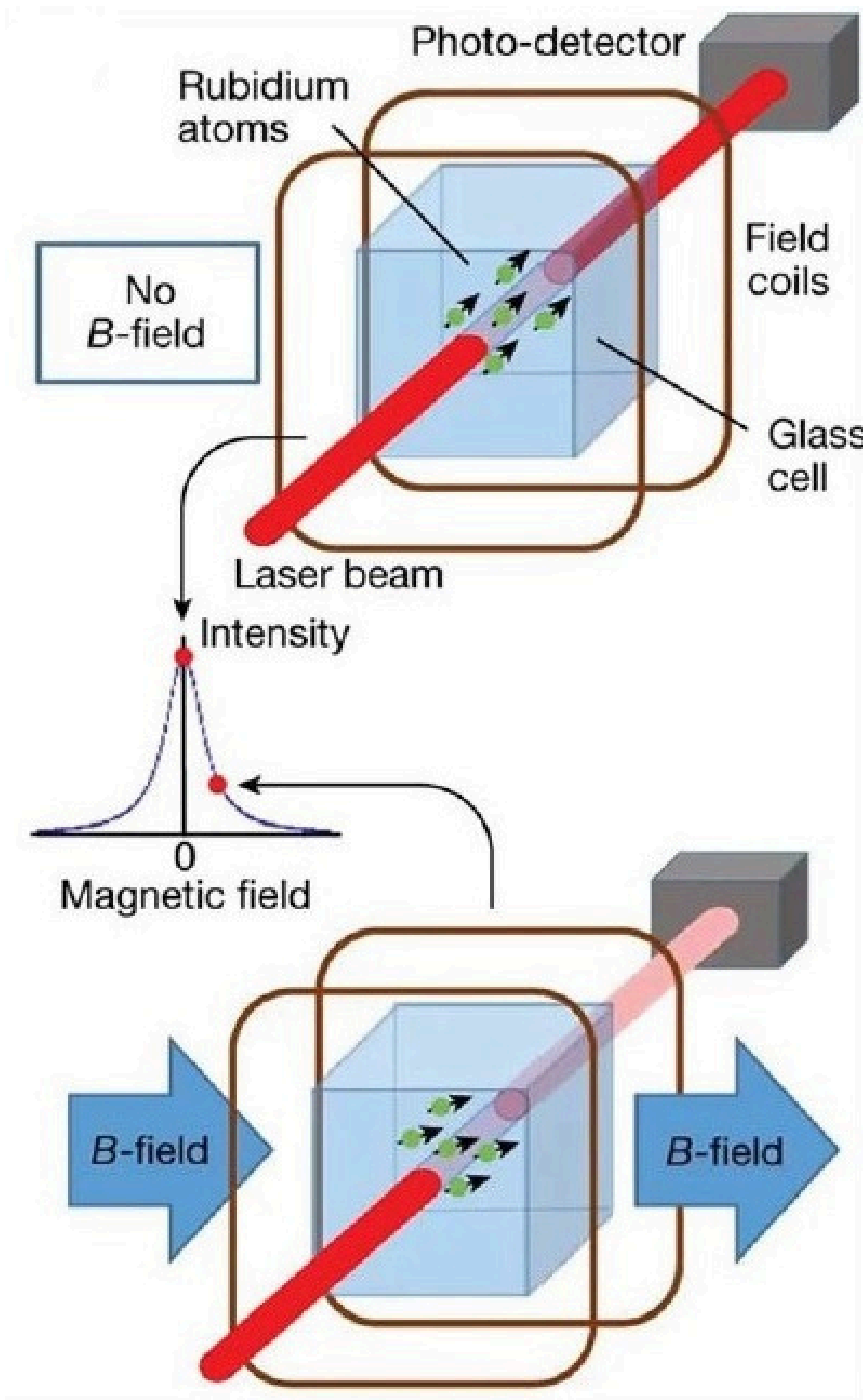


Luz de comprimento de onda de 795 nm. induz a transição D1 entre os níveis de energia L=0 e S=1/2 do estado atómico fundamental, e o nível L=1 e S=1/2 do primeiro estado excitado.

Aplicando um campo magnético muito fraco (inferior a 10 nT), há um desdobramento dos níveis hiperfinos do estado fundamental e do primeiro estado excitado. Usando luz incidente com polarização circular positiva, a absorção só ocorre se o valor de m aumentar de uma unidade. Ao desexcitar, este processo não é inteiramente invertido (as regras de seleção na emissão espontânea são diferentes) e há uma acumulação de população num estado com m=2. Os átomos ficam “presos” no estado com m=2 e deixa de ser possível a absorção de luz. O vapor fica transparente à luz laser. Este efeito chama-se optical pumping

Sensores Quânticos

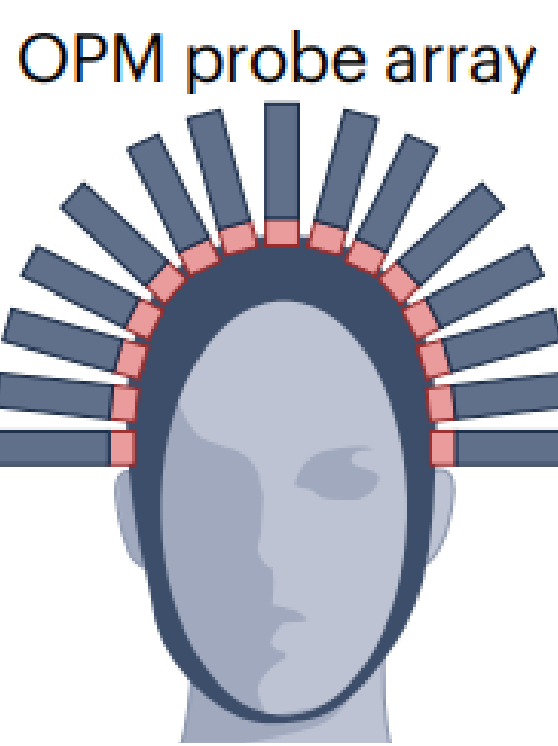
A acumulação de população no estado hiperfino m=2 do estado eletrónico fundamental causa uma elevada polarização de spin no vapor de rubídio. Esta polarização é perturbada pelo campo magnético exterior que se pretende medir, permitindo a sua medida com uma sensibilidade muito elevada.



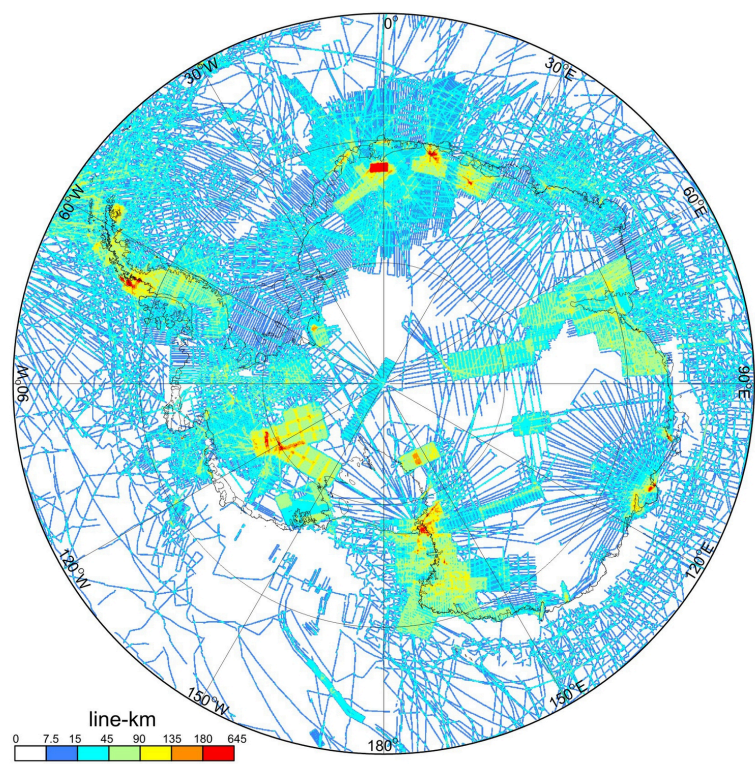
Aplicações

Biomagnetismo

Utilização em técnicas médicas como a magnetoencefalografia cuja finalidade é a medição de campos magnéticos produzidos pelo cérebro.



Sistemas de Navegação



Utilização de OPMs em sistemas de navegação sem recurso a GPS, medindo pequenas variações do campo magnético terrestre.

OPMs VS outros sensores

	Sensibilidade $fT/\sqrt{Hz}$
OPM	1 ~ 20
SQUID	~ 1
Sensor NV Diamante	~ 100

Os OPMs revelam-se muito promissores como futuros sensores substitutos dos convencionais, contudo ainda se encontram desafios em aberto como o encontrar estratégias para mitigação do alto ruído associado aos mesmos.

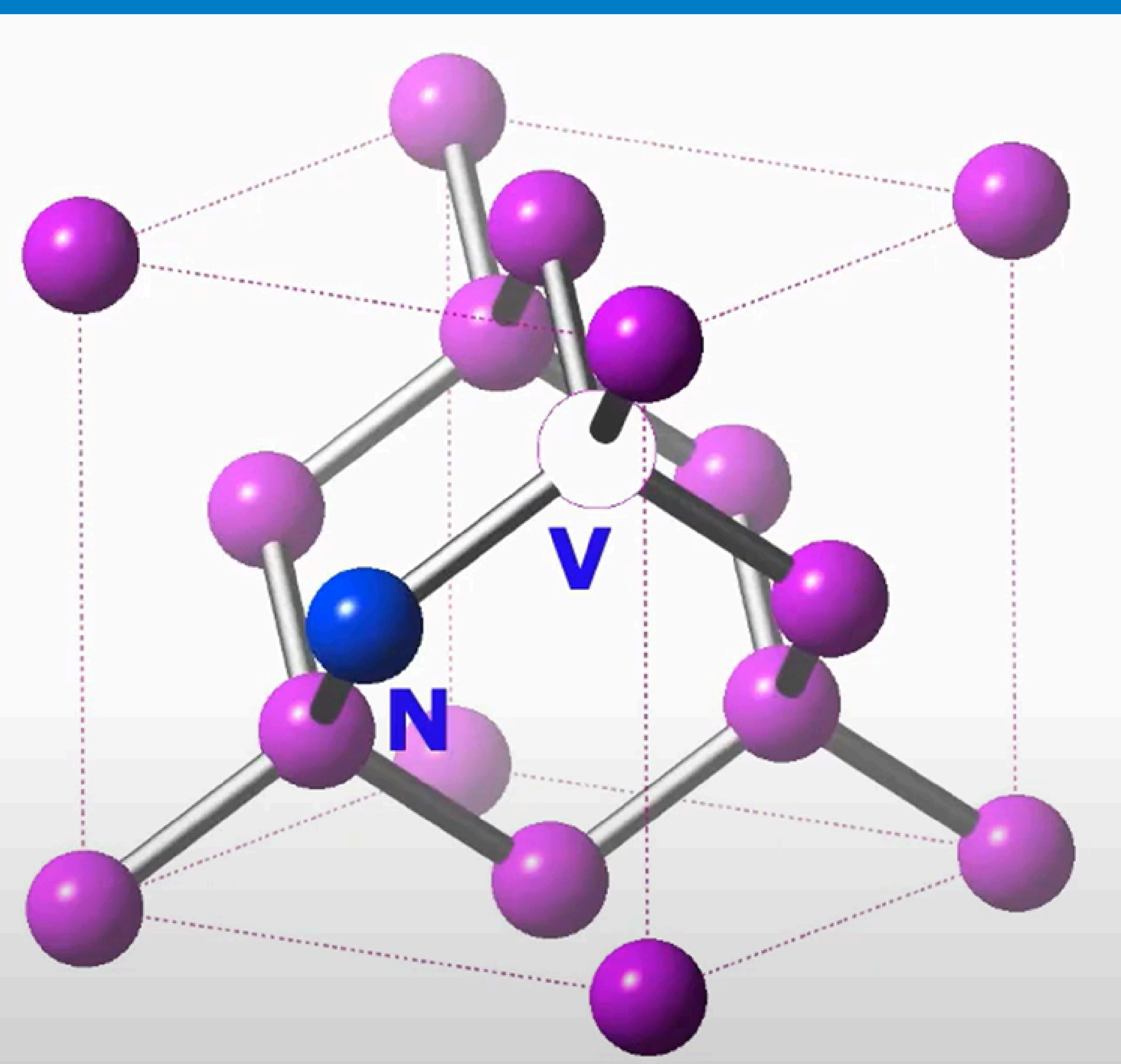
Sensores magnéticos de diamante com centro NV

Gonçalo Ramos

Universidade de Coimbra

Um centro NV é um defeito no diamante que consiste na substituição de um átomo de carbono por um átomo de azoto, associado a uma lacuna.

No estado fundamental, o centro NV forma um tripleto de spin ($S = 1$) com 3 subníveis de energia: $m_s = 0$ e $m_s = \pm 1$, sendo a energia do estado $m_s = 0$ menor do que a de $m_s = \pm 1$, devido ao campo cristalino. Constitui um qubit cujos estados de spin podem ser manipulados através de radiação de frequência adequada.



Campo Magnético Nulo

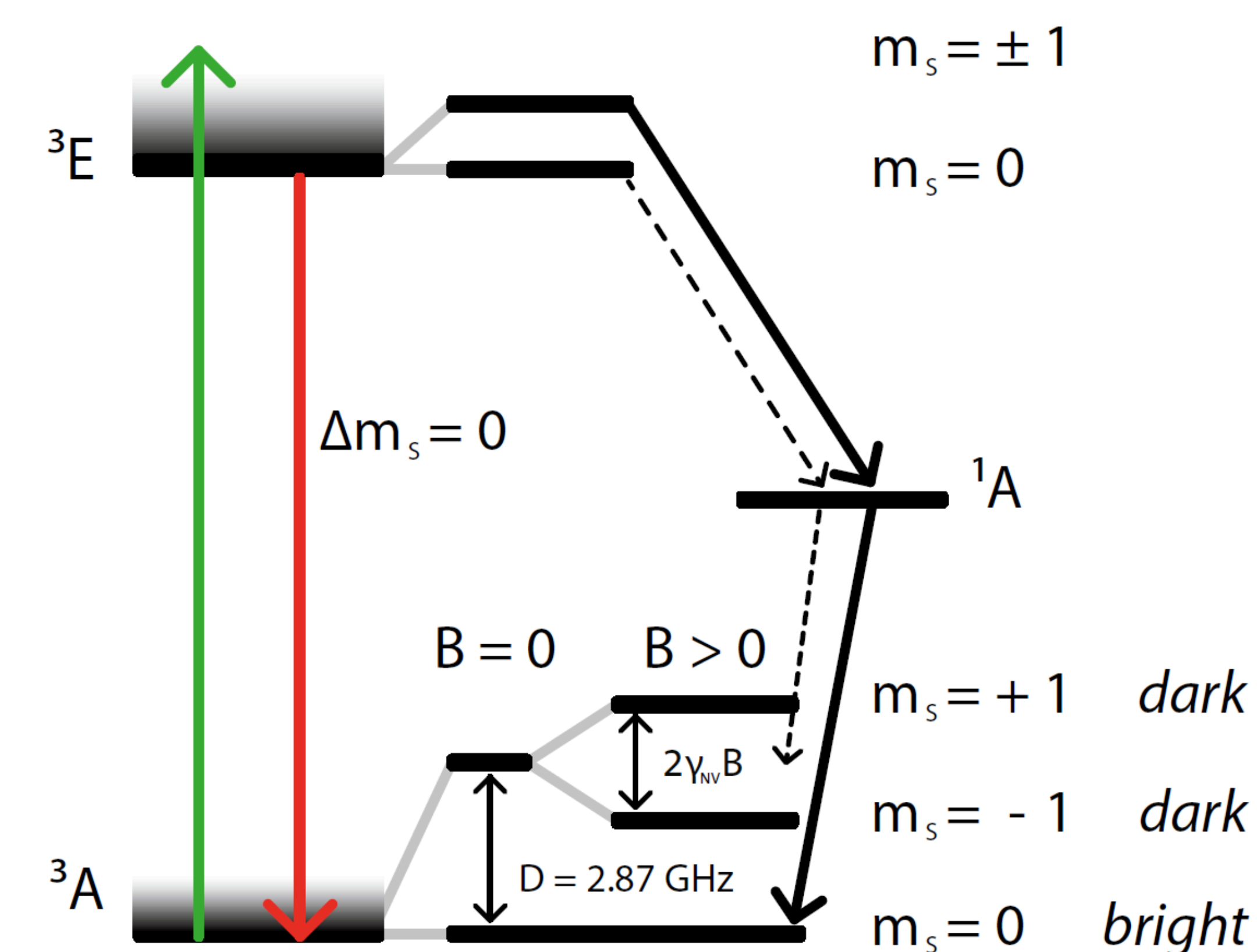
A transição de $m_s = 0$ a $m_s = \pm 1$ pode ser induzida com radiação de microondas de frequência $D = 2,87$ GHz.

Adicionalmente, uma excitação com luz verde permite popular o estado $m_s = \pm 1$ no primeiro estado eletrónico excitado. Este estado $m_s = \pm 1$ decai para o estado fundamental $m_s = 0$, diretamente ou através de um estado intermédio. Sendo esse estado intermédio de vida longa, a população do estado $m_s = 0$ do estado fundamental aumenta, originando uma fluorescência intensa na frequência de ressonância $D = 2,87$ GHz.

Campo magnético não-nulo

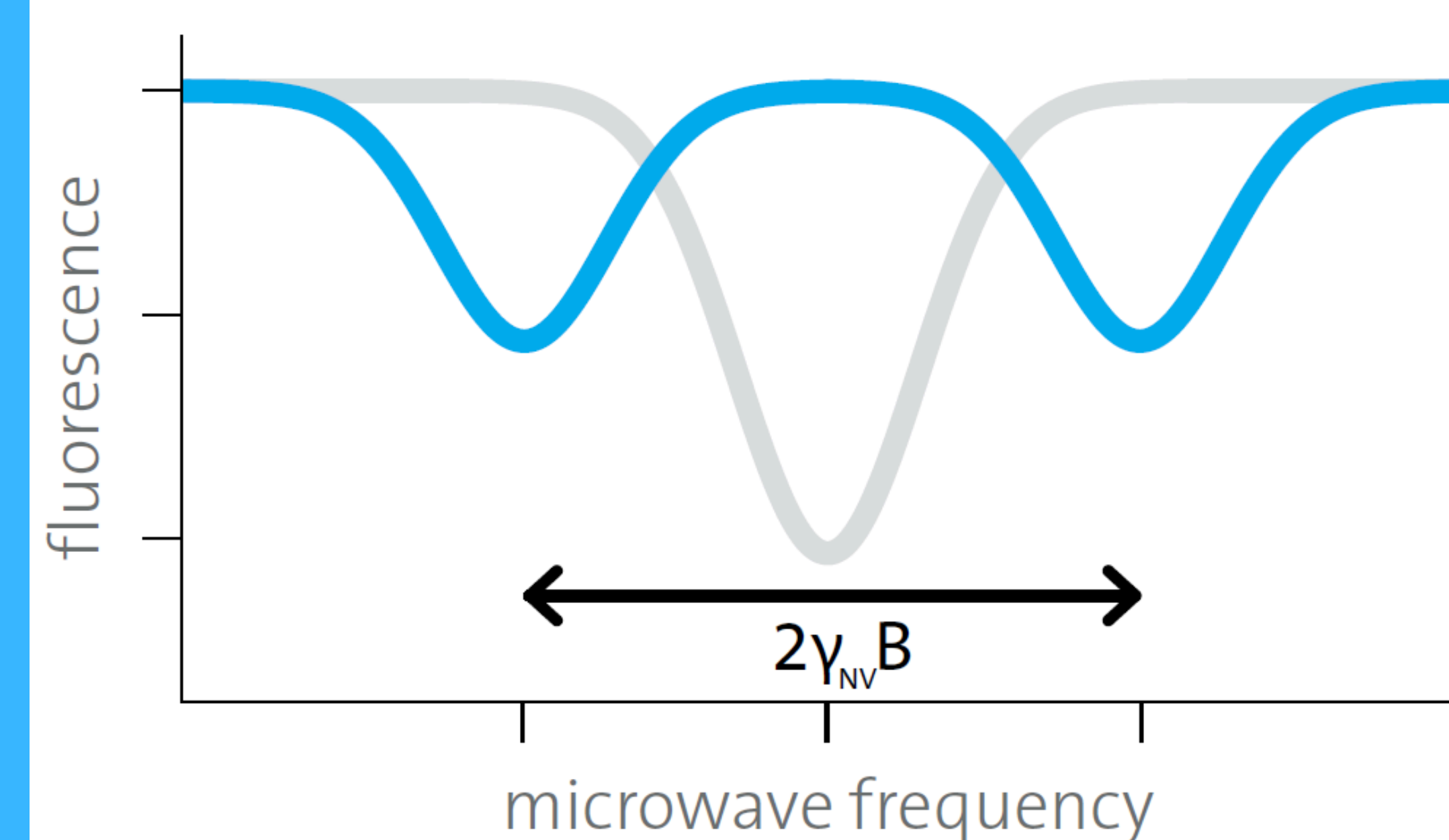
Para $B > 0$, os níveis $m_s = \pm 1$ separam-se, sendo a separação proporcional ao campo magnético (efeito de Zeeman).

Sensores Quânticos



Camo pode ser medido o campo magnético?

A separação em energia os níveis $m_s = \pm 1$ na presença de um campo B é medida experimentalmente pela correspondente separação entre as frequências de ressonância, o que permite determinar o campo magnético com elevada sensibilidade.



Uma vantagem importante destes sensores é terem dimensões atômicas, com um confinamento da função de onda eletrónica da ordem de alguns nanómetros. Além disso, os centros podem ser formados junto à superfície do diamante. Estes dois aspetos tornam possível uma resolução espacial destes sensores da ordem dos nanómetros.

Vantagens:

- Alta sensibilidade ($\text{pT}/\sqrt{\text{Hz}}$);
- Alta resolução (nm);
- Funciona a temperatura ambiente;
- Estados de spin com coerência elevada.
- Biocompatível;
- Leitura de saída simples (ótica);
- Mede valores absolutos;
- Não intrusivo para a amostra.



GRAVÍMETROS QUÂNTICOS

Francisco Ferreira

Universidade de Coimbra

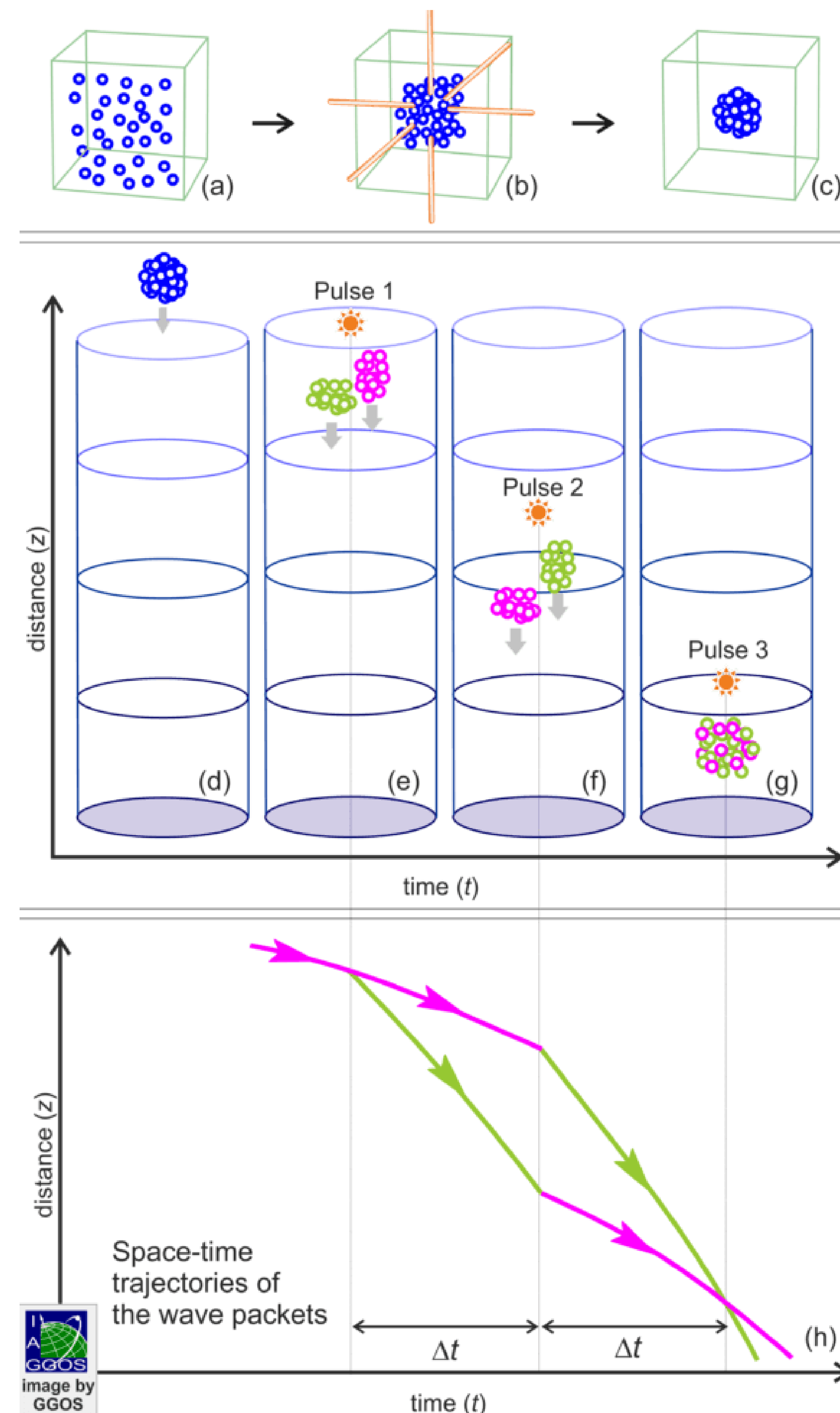
Gravímetros são instrumentos usados para medir a aceleração gravítica num determinado ponto da superfície terrestre.

Os gravímetros quânticos fazem-no tirando partido das propriedades ondulatórias da matéria.

AQG: Como Funciona?

Na figura, uma nuvem de átomos (geralmente Rubídio-87) é confinada numa câmara de vazio (a) e depois arrefecida por lasers a temperaturas da ordem de microkelvin. (b). A estas temperaturas os átomos movem-se devagar e comportam-se como ondas de matéria que podem ser manipuladas com laser.

A nuvem de átomos é libertada permitindo que caia em queda livre sob a ação da gravidade (d) e são expostos durante a queda a uma sequência de três pulsos laser



Um gravímetro quântico usa interferometria atômica para medir a aceleração da gravidade. É muito sensível a flutuações do campo gravítico.

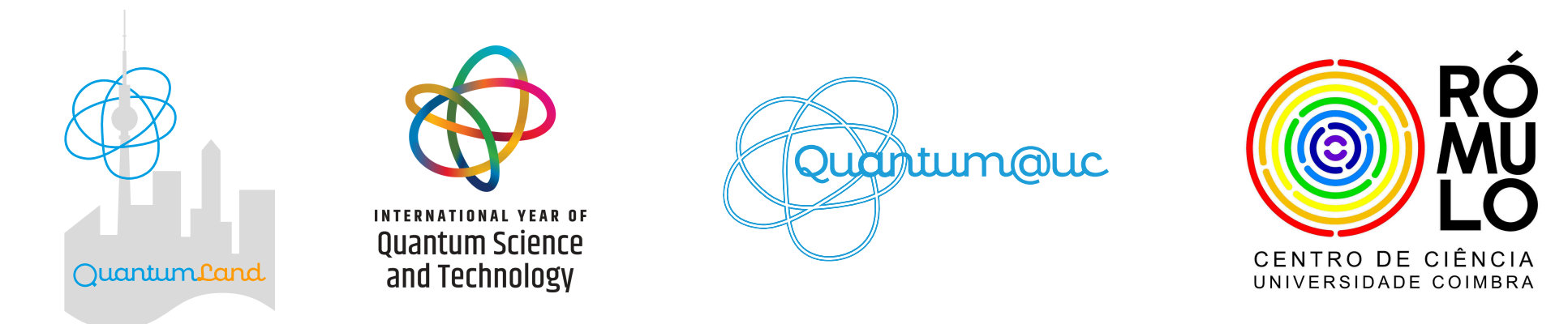
Sensores Quânticos

Interferometria Atômica

- Na figura, em (e), o primeiro pulso transforma a função de onda de cada átomo numa sobreposição de dois estados.
- Os dois pacotes de onda atômicos seguem trajetórias diferentes e sentem o campo gravítico de forma diferente. A diferença de fase entre os dois pacotes de onda vai-se acumulando.
- Um segundo impulso laser inverte os estados. (f)
- O último pulso recompõe ambos os estados, permitindo a interferência entre eles. (g)
- O padrão de interferência é medido através da deteção do número de átomos em cada estado quântico final. (h)
- A diferença de fase entre os dois é proporcional à aceleração gravitacional g e constitui uma medida de g .

Sensibilidade a gradientes de campo gravítico

- O gravímetro quântico pode funcionar em contínuo e medir não só valores absolutos mas também variações da aceleração gravítica.
- O padrão de interferência é muito sensível a pequenas variações do campo gravítico.



Perspetivas atuais e futuras

Os gravímetros quânticos estão em desenvolvimento há 30 anos, começando recentemente a ser comercializados.

Um dos primeiros a consegui-lo com sucesso é o "Absolute Quantum Gravimeter" (AQG) da Muquans (Exail).

O protótipo do "Differential Quantum Gravimeter" da Exail demonstrou conseguir detetar estruturas subterrâneas fiavelmente e mais rapidamente do que gravímetros quânticos anteriores.

Evoluindo neste sentido, os gravímetros quânticos poderão melhorar drasticamente o campo da gravimetria!

Poema da Eterna Presença

Estou, nesta noite cálida, deliciadamente estendido sobre a relva,
de olhos postos no céu, e reparo; com alegria,
que as dimensões do infinito não me perturbam.
(O infinito!

Essa incomensurável distância de meio metro
que vai desde o meu cérebro aos dedos com que escrevo!)

O que me perturba é que o todo possa caber na parte,
que o tridimensional caiba no dimensional, e não o esgote.

O que me perturba é que tudo caiba dentro de mim,
de mim, pobre de mim, que sou parte do todo;
E em mim continuaria a caber se me cortassem braços e pernas,
porque eu não sou braço nem sou perna.

Se eu tivesse a memória das pedras,
que logo entram em queda assim que se largam no espaço
sem que nunca nenhuma se tivesse esquecido de cair;
se eu tivesse a memória da luz,
que mal começa, na sua origem, logo se propaga,
sem que nenhuma se esquecesse de propagar;
os meus olhos reviveriam os dinossáurios que caminharam sobre a Terra,
os meus ouvidos lembrar-se-iam dos rugidos dos oceanos que engoliram continentes,
a minha pele lembrar-se-ia da temperatura das geleiras que galgaram sobre a Terra.
...

Tudo se passou defronte de partes de mim.
E aqui estou eu feito carne para o demonstrar,
porque os átomos da minha carne não foram fabricados de propósito para mim.
Já cá estavam.
Estão:
E estarão:

António Gedeão

A conta é infinita.

(até pode ser de areia
mas é preferível ser de pedaços de poema)
de cada vez que se lê
apenas um pedaço é observado
em probabilidade que cresce devagar
não se vê exatamente o crescer
nunca se vê exatamente o crescer de nada vivo
é ainda provável
que este pedaço se ilumine ao ser observado
que se alterne aqui ou ali
para agradar
e que goste

Joana Espain

Uma onda que ri

Menos dimensões à solta de não saber
não deslizar pelas lâminas circulares
entre uma e outra ir saltando sem violino
em ritmos de eco
rir com ela
nos seus modos de ondulação
ouvindo o reflexo do fundo dos poços
na exacta inclinação das variáveis
que se deixam observar
e ela ri-se
com a rotação de todos os polegares uma só onda
inteira de mundo
na exata probabilidade de nos amar

Joana Espain

Lentamente chegando este instante

de a deixar passar a um espaço húmido e quente
sempre que queira, não a orientar
ser mais leve que o som que a traz ao abrir
tocar na informação sem fazer força
com um poema, um ramo de cada vez,
e a meio a música em fractal
em instante que ainda a contenha
para lá de a ter tido
escrevesse ela a sua melhor história
em todas as células
usasse vida em vez de papel
e assinatura de riso no final
para evitar o plágio

Joana Espain



Ficha Técnica

Exposição QuantumLand

Data 13 de março a 9 maio de 2025

Inauguração 13 de março às 17h

Local Rómulo - Departamento de Física, Universidade de Coimbra

Organização Rómulo e Quantum@UC

Direção Helena Alberto e Constança Providência

Coordenação Científica Helena Alberto e Sagar Pratapsi

Design Gráfico Pérola do Mar (Rita Wolters)

Ilustração A Grande Revolta dos Gatos de Schrödinger, Sagar Pratapsi e Joana Esteves

Apoio Técnico Felipe Demégio

Atividade inserida na programação da
XXVII Semana Cultural da Universidade de Coimbra