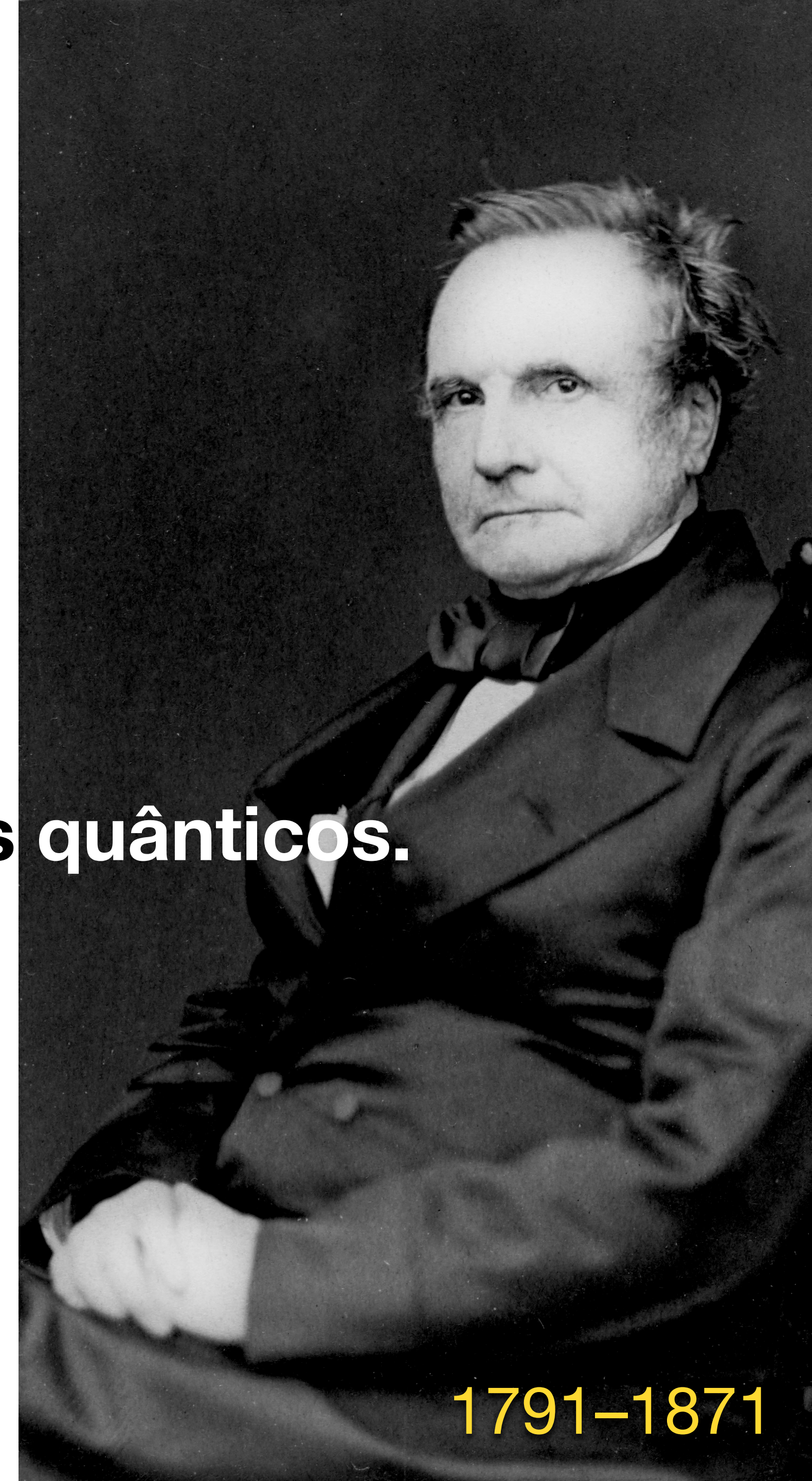


Física — 12.º ano

14 — Infra-vermelhos na guerra. Computadores quânticos.

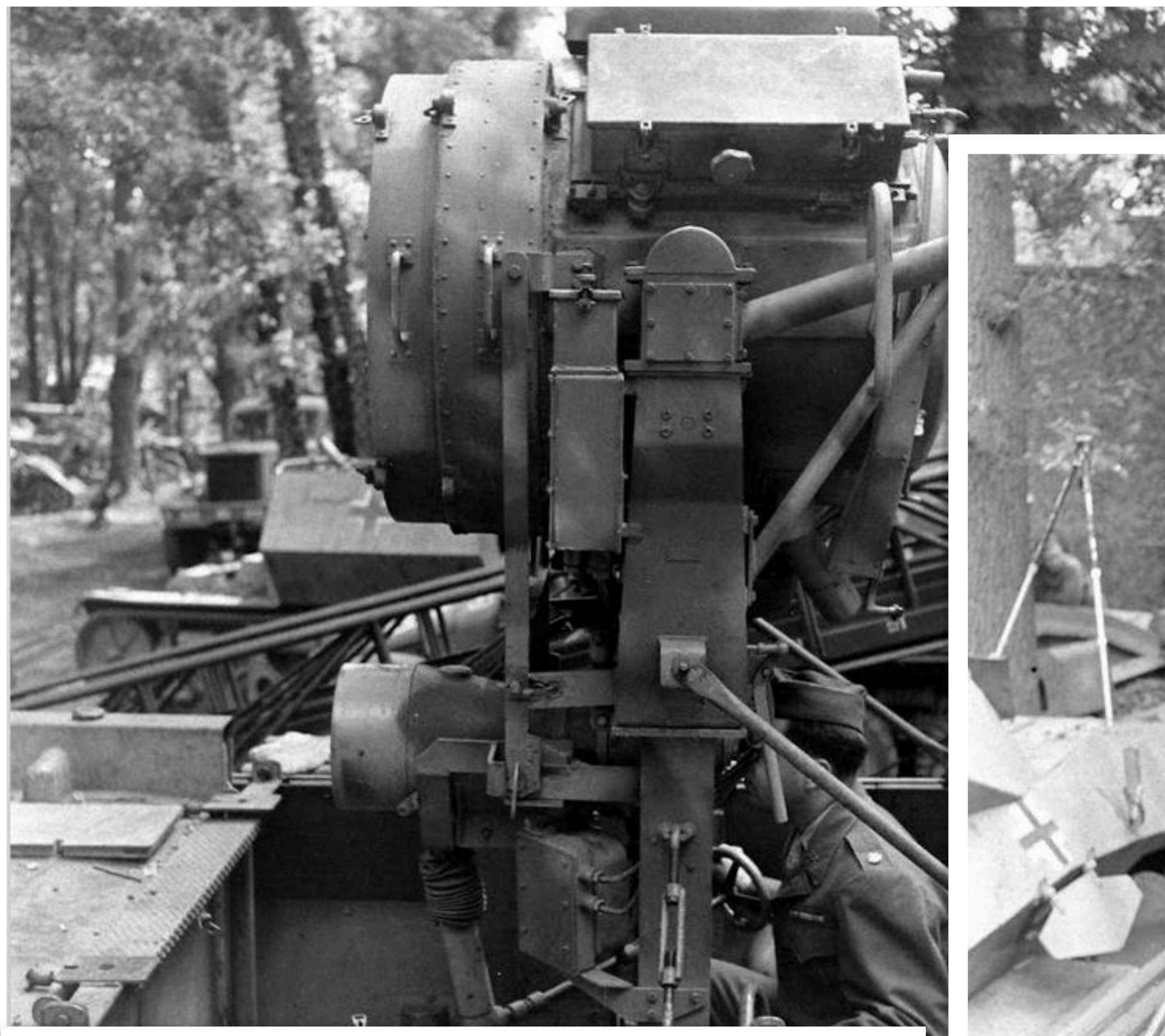


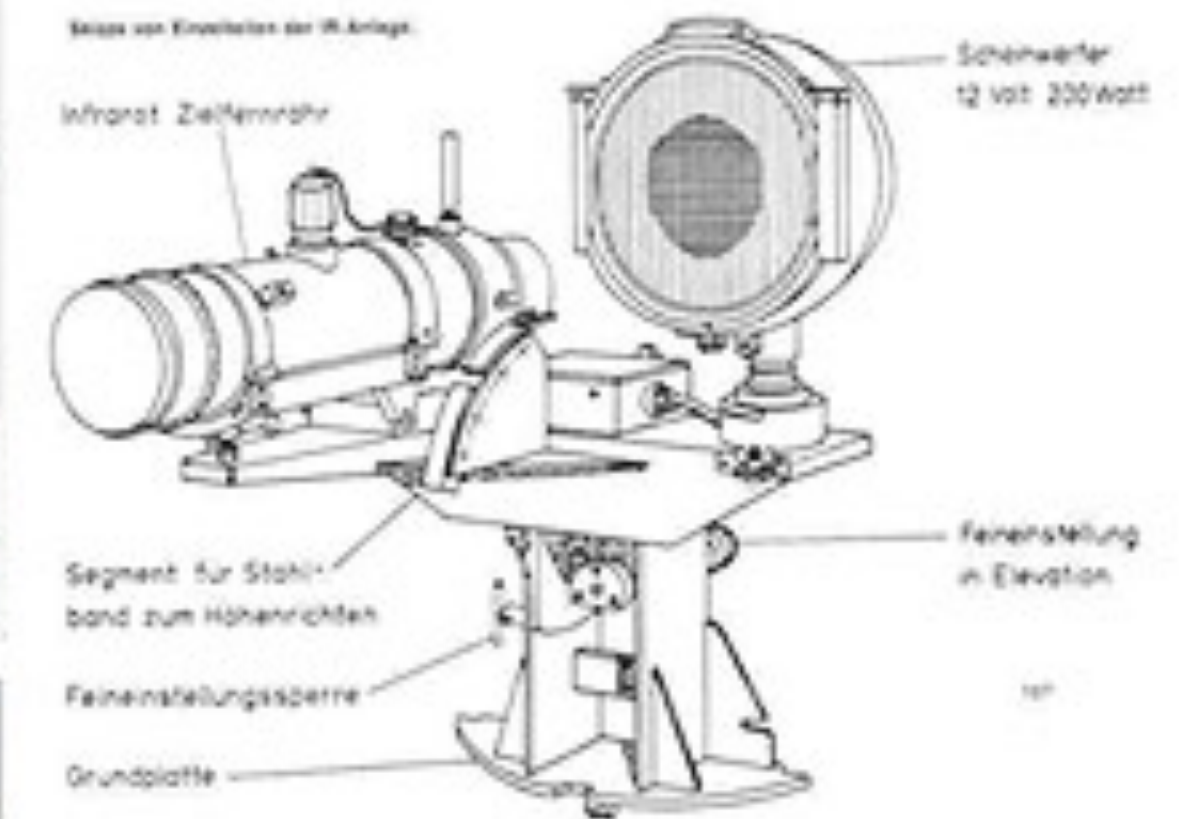
José Pedro do Amaral zp.amaral@colegiodestomas.com



1791–1871

IV (NIR) na Segunda Grande Guerra









Alemanha e as anilinas

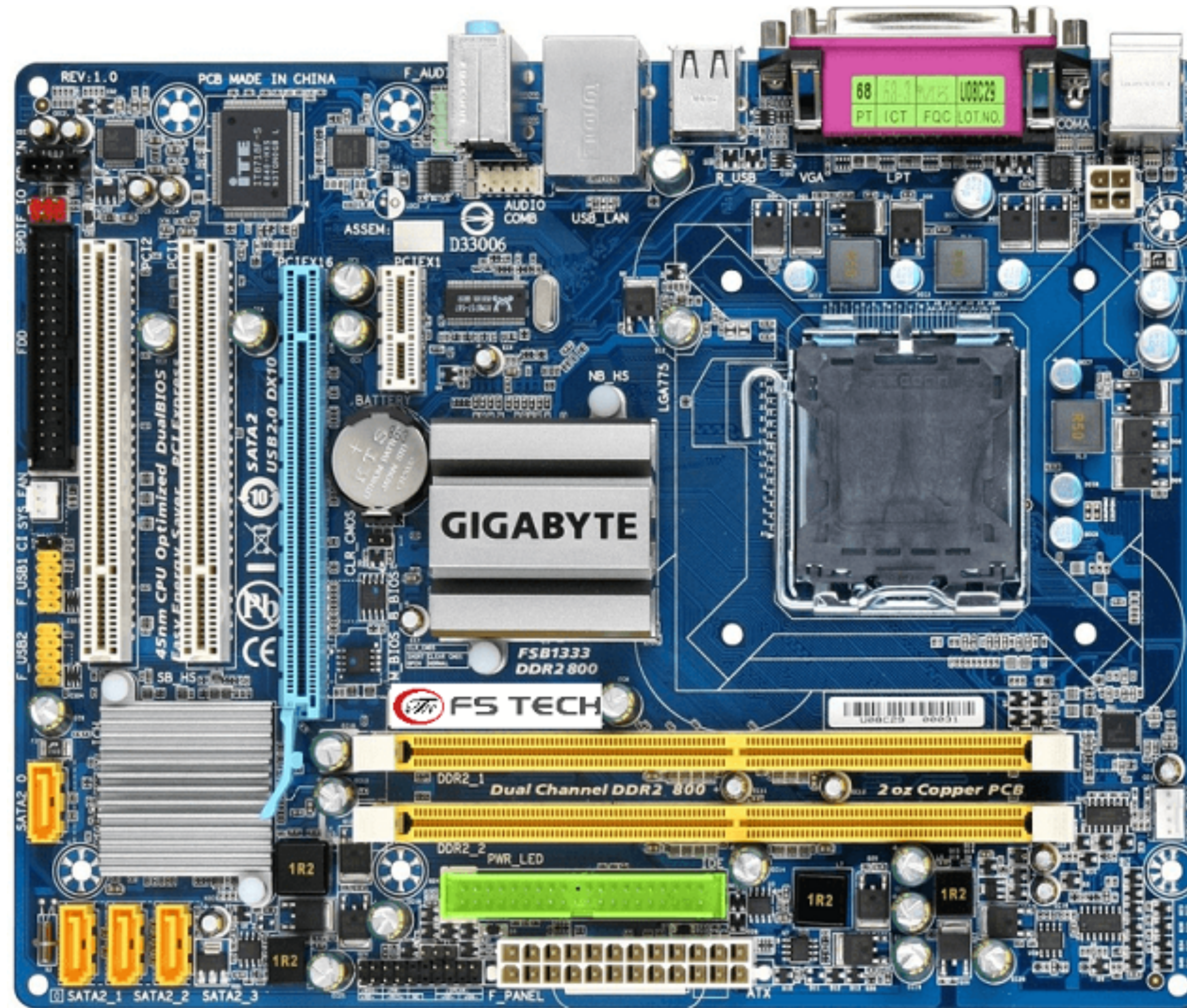
tinta de anilina preta

Leibermuster



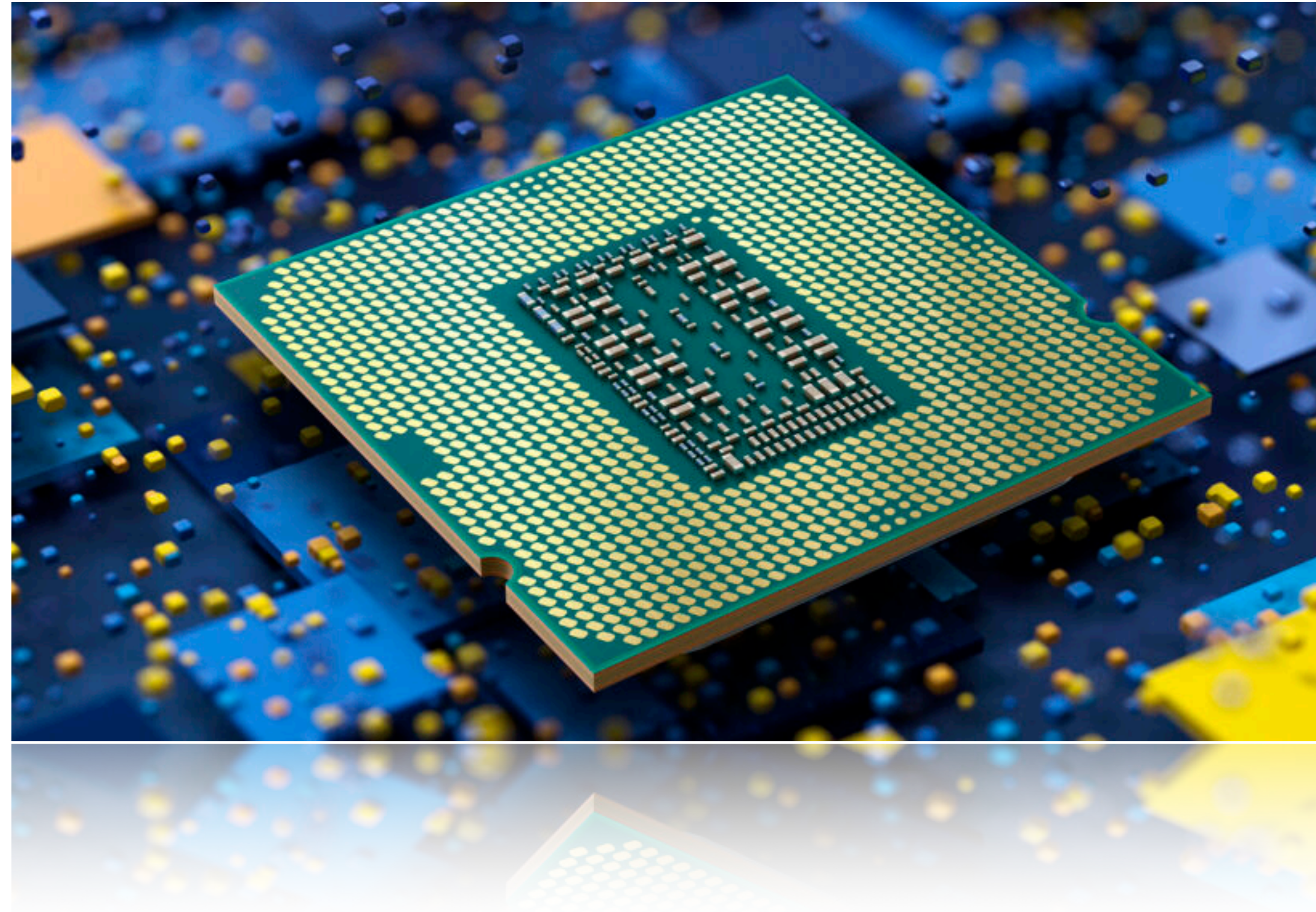
foto tirada pela RAF com
filme de infravermelhos a um
sítio de lançamento de V1

Computadores (clássicos)



«motherboard»

- A «motherboard», placa mãe, placa de circuitos principal é a placa que integra e conecta todos os outros componentes de um computador.



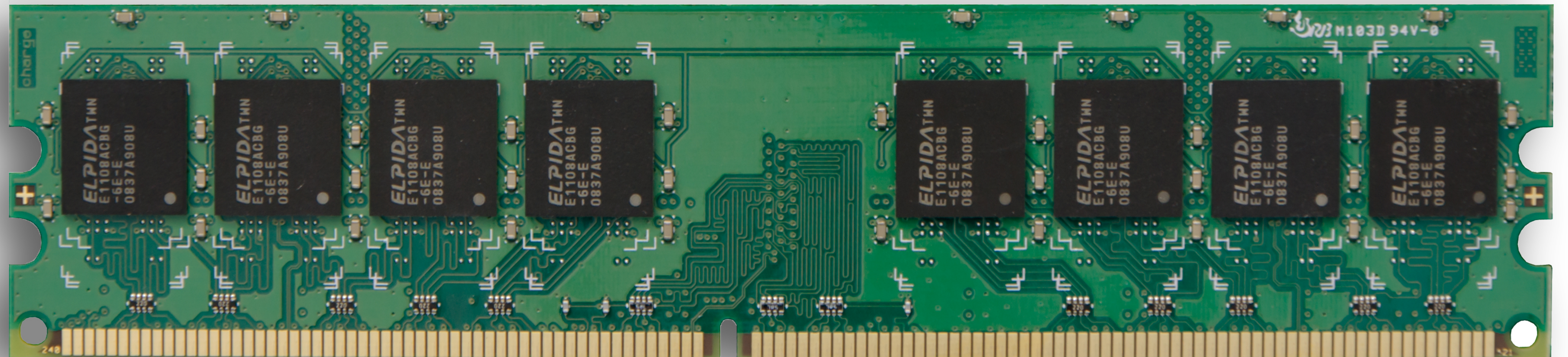
CPU

- A CPU (Unidade Central de Processamento) é o componente responsável por executar as instruções dos programas: operações aritméticas e lógicas, controle do fluxo de execução e gestão das transferências de dados entre os restantes componentes do computador.



discos HDD (esquerda) e SSD (direita)

- O disco é o componente onde a informação é gravada de forma persistente. Dependendo da organização do sistema operativo, pode conter os dados do utente, os ficheiros do próprio sistema operativo e ainda o espaço reservado à memória virtual, de que falaremos de seguida.



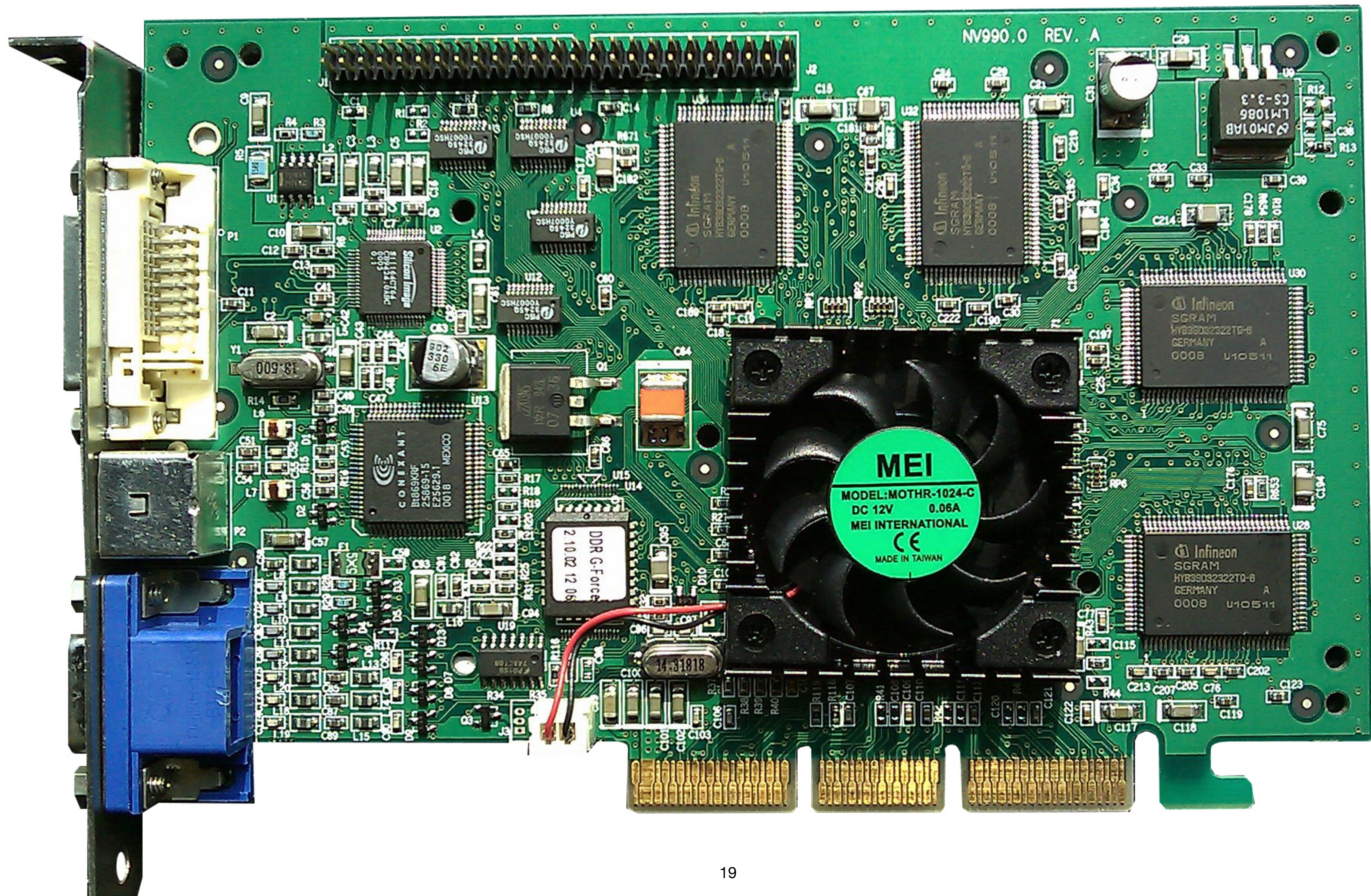
RAM

- RAM, memória de acesso aleatório é a memória onde estão os programas em execução. O programa pode ler e escrever informação de forma não-sequencial (daí o termo aleatório) de forma rápida mas lábil, pois o seu conteúdo desaparecerá com uma interrupção da corrente eléctrica. Quando a RAM disponível é insuficiente, o sistema operativo pode usar espaço no disco como extensão temporária de memória (a tal memória virtual).



ROM

- A ROM (memória só de leitura) é a memória onde residem as instruções de arranque do computador. Isto é, contém as instruções que preparam o sistema para começar a carregar o sistema operativo. Nos computadores mais recentes, a ROM como componente separado tende a desaparecer: é substituída por memória flash integrada na placa, que cumpre a mesma função mas pode ser actualizada, e cuja lógica de arranque trabalha em conjunto com uma partição dedicada no disco.



GPU

- A GPU (Unidade de Processamento Gráfico) é um processador dedicado, dotado de memória própria de alta largura de banda, altamente eficiente na execução de determinadas operações matemáticas. Inicialmente concebida para o processamento de imagem e gráficos em tempo real, evoluiu para um papel mais amplo: a sua arquitectura massivamente paralela — com milhares de núcleos de processamento — torna-a adequada a executar simultaneamente muitas tarefas de computação especializada que complementam as da CPU.



placa *Ethernet*

- A placa de rede Ethernet é o componente que estabelece a ligação física por cabo do computador a uma rede local ou à Internet. Incorpora uma porta à qual se liga o cabo, e implementa o protocolo Ethernet (o padrão que rege a transmissão de dados nesse meio físico) sobre o qual assentam protocolos de nível superior como o TCP/IP, responsáveis pela comunicação entre computadores.



placa WiFi

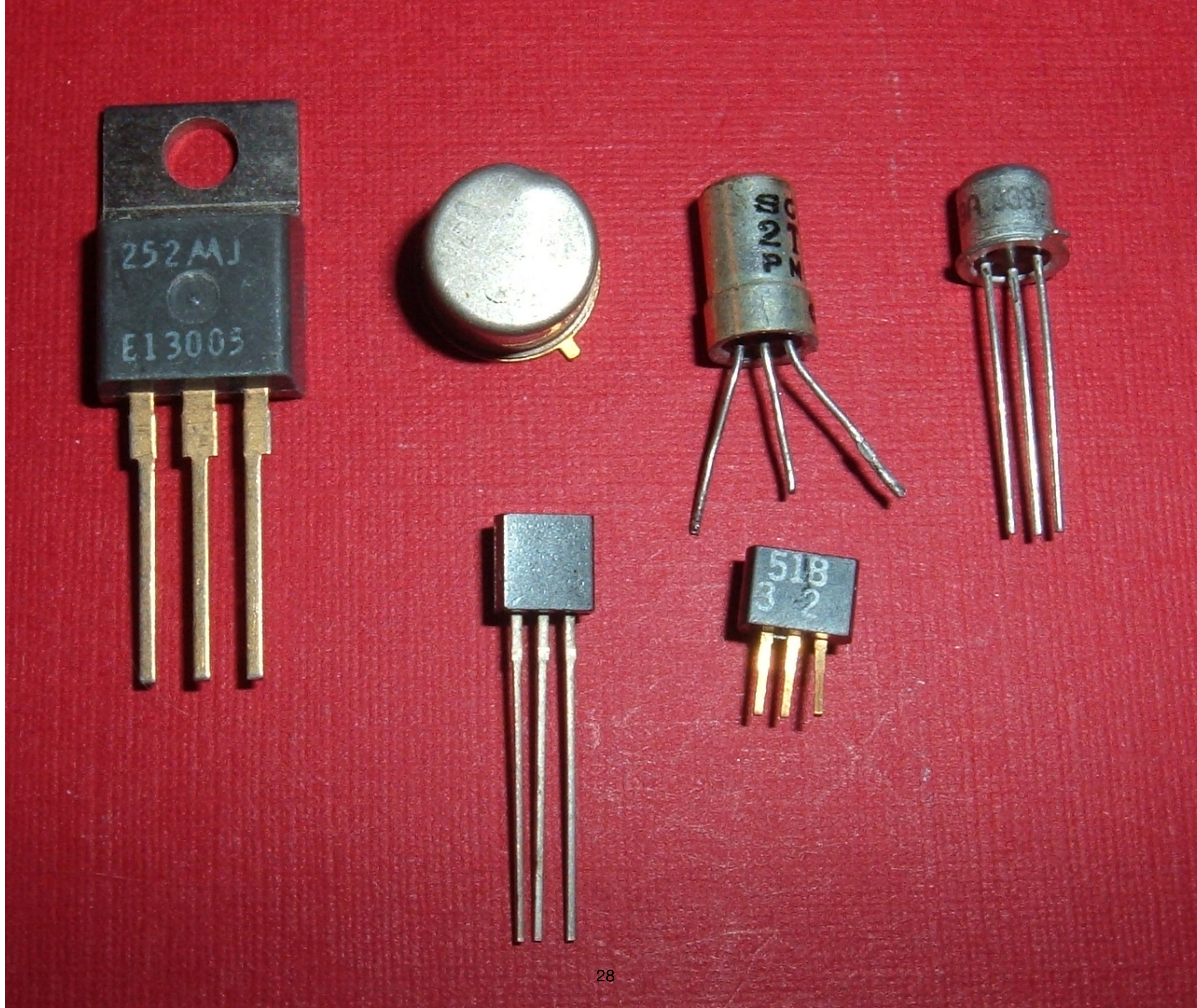
- A placa de rede WiFi é o componente que estabelece a ligação sem fios do computador a um ponto de acesso da rede local, por ondas de rádio. Incorpora um sistema de rádio com antena emissora-receptora e implementa o protocolo IEEE 802.11 (o padrão que define a transmissão de dados por rádio neste contexto) sobre o qual assentam protocolos de nível superior como o TCP/IP, responsáveis pela comunicação entre sistemas.

e muitos outros componentes...

Válvulas e transístores



válvulas



transistores

- A comparação entre válvulas (*vacuum tubes*) e transístores é uma comparação entre duas eras e duas abordagens da electrónica.
- As **válvulas**, como o tríodo, surgiram no início do século XX e funcionam controlando o fluxo de electrões no vácuo, entre um cátodo aquecido e um ânodo, com uma grelha de controlo intermédia. Esse aquecimento implica consumo elevado de energia, geração de calor e dimensões relativamente grandes. Em contrapartida, as válvulas toleram bem sobretensões, têm uma resposta intrinsecamente suave à saturação (o que as torna apreciadas em áudio) e são menos sensíveis a radiação electromagnética.
- Os **transístores**, como o transistor bipolar ou os de efeito de campo, surgiram a meio do século XX e baseiam-se em semicondutores. Não requerem aquecimento, são muito mais pequenos, eficientes e duráveis, e permitem a integração em larga escala que originou os circuitos integrados e a electrónica moderna. Oferecem maior estabilidade, menor consumo e maior fiabilidade a longo prazo.
- No entanto, há diferenças subtis no comportamento: os transístores, quando levados ao limite, produzem distorções mais abruptas, mas as válvulas tendem a introduzir distorções harmónicas suaves consideradas «musicais». Por isso, apesar de tecnologicamente ultrapassadas, as válvulas continuam a ser usadas em nichos como amplificadores de guitarra e áudio de alta-fidelidade.
- Os transístores venceram pela eficiência, miniaturização e custo, mas as válvulas mantêm nicho onde o seu «defeito» é, paradoxalmente, a sua maior virtude.

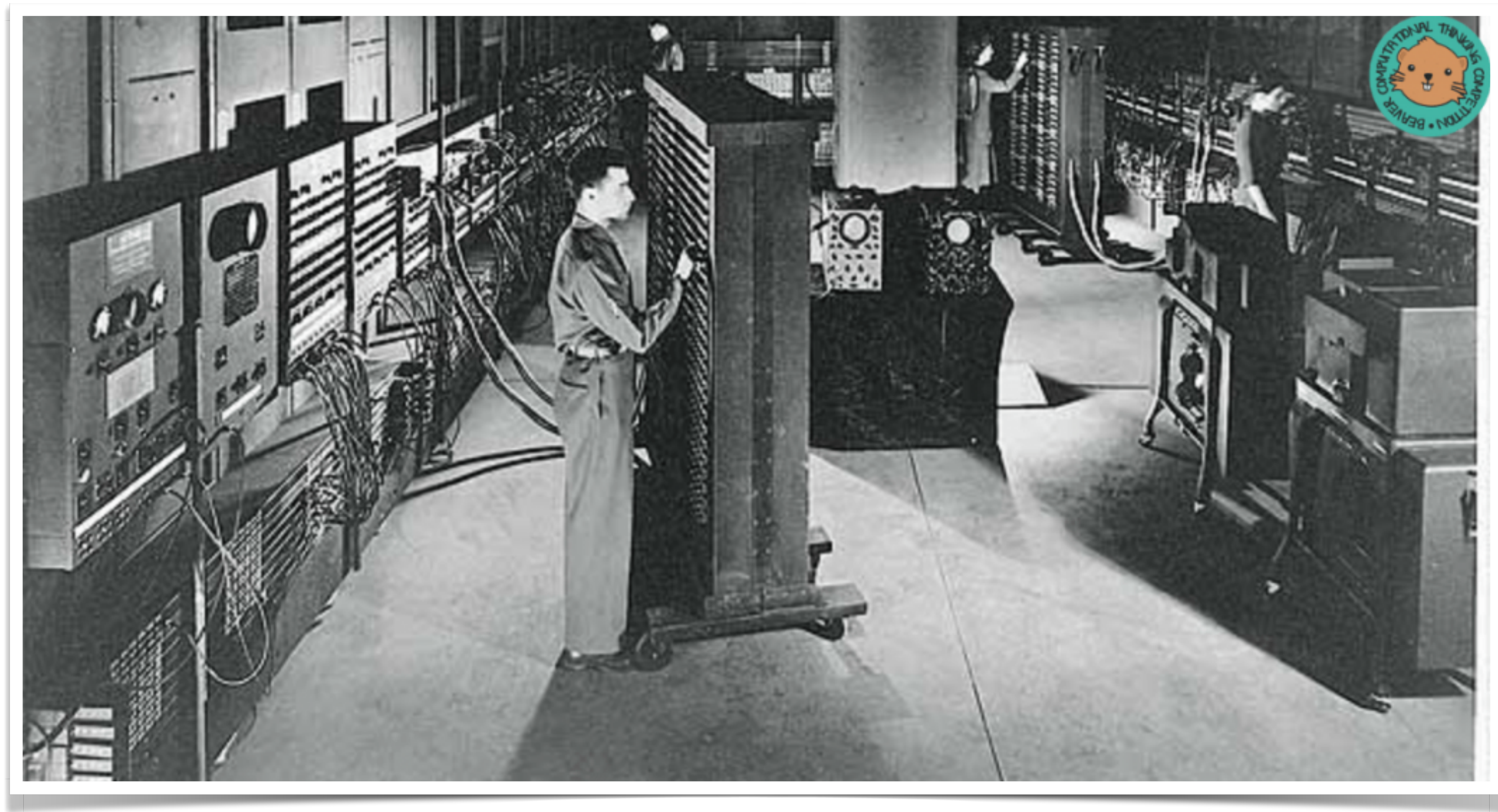
O que fazem concretamente

Num circuito desempenham três funções principais:

1. **Amplificação.** Um sinal fraco (por exemplo, de um microfone) entra → o dispositivo controla uma corrente maior → à saída tens o mesmo sinal, mas mais forte.
 - Na válvula: a grelha controla o fluxo de electrões no vácuo.
 - No transístor: a base (ou gate) controla a corrente entre colector-emissor (ou dreno-fonte).
2. **Comutação** (interruptor electrónico). Podem funcionar como um interruptor sem partes móveis:
 - a. desligado → não passa corrente (0)
 - b. ligado → passa corrente (1)

➡ E isto é a base de toda a electrónica digital.
3. **Modelação de sinal.** Podem modificar formas de onda (filtragem, oscilação, distorção, mistura, etc.).

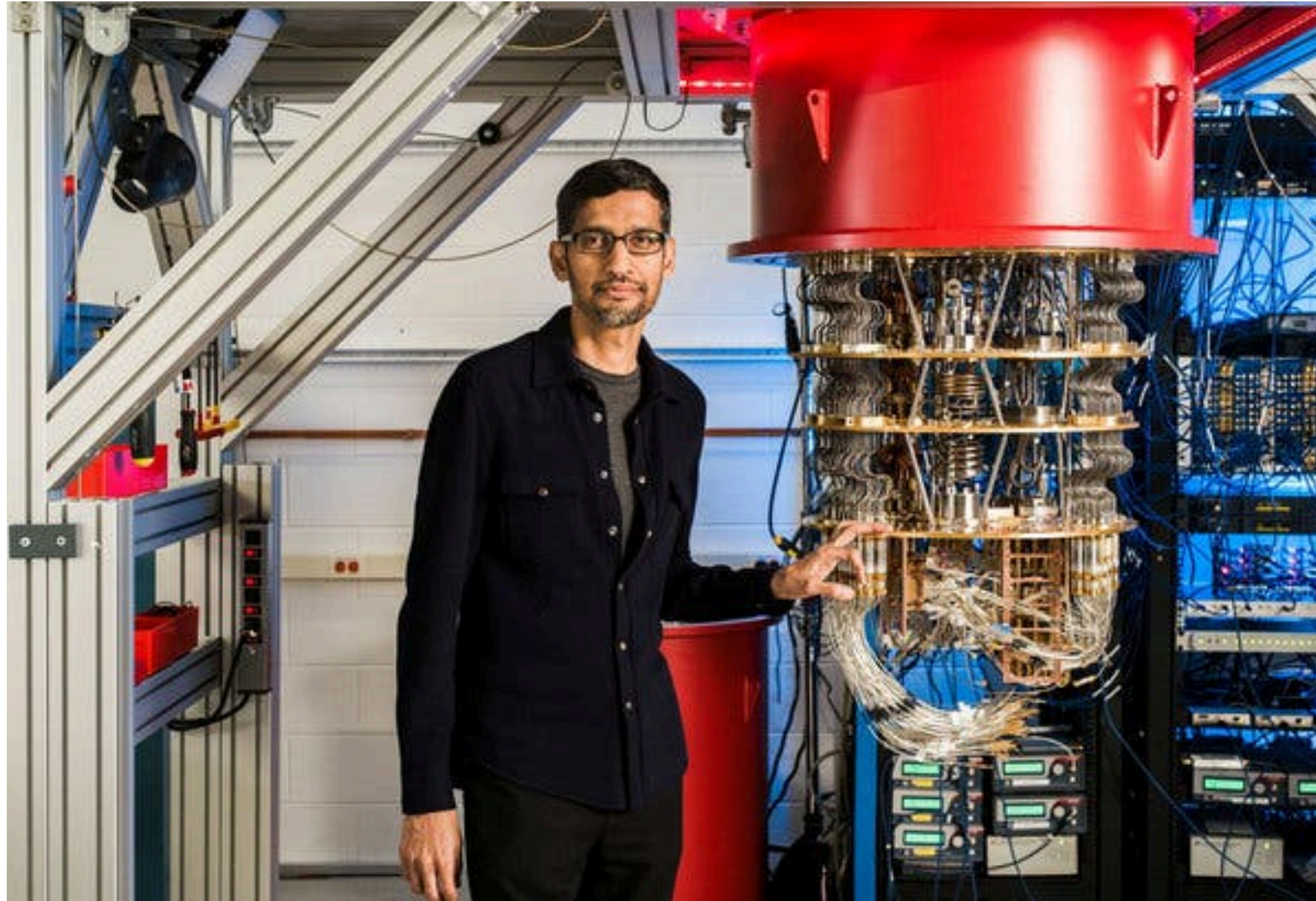
18.000 válvulas

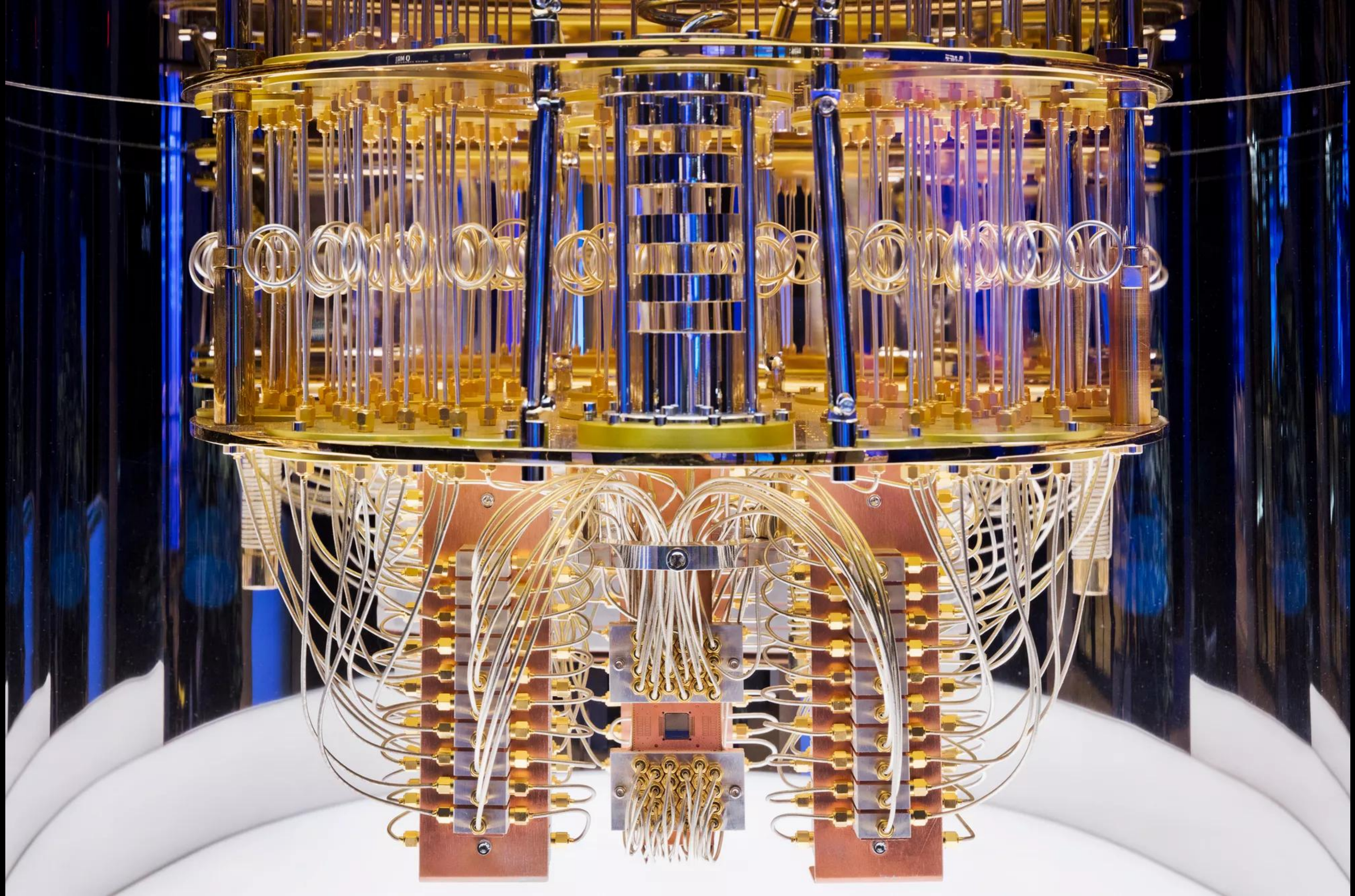


ENIAC Electronic Numerical Integrator and Computer



Computadores (quânticos)





- Há várias plataformas físicas para computação quântica, e os fótons são apenas uma delas:
 - Iões aprisionados (*trapped ions*): *qubits* codificados em estados electrónicos de iões, manipulados por lasers
 - Transmons / circuitos supercondutores — *qubits* de microondas a temperaturas de milikelvin; é a plataforma do Google, IBM e outros
 - Centros de cor em diamante (NV, Nitrogen-Vacancy centres): *spins* electrónicos em defeitos cristalinos
 - Qubits de fótons: onde o *emaranhamento* via SPDC (*Spontaneous Parametric Down-Conversion*) é de facto central

O emaranhamento de fótons é porém indispensável na comunicação quântica e criptografia quântica — aqui sim, os pares produzidos por SPDC são a ferramenta dominante.

Exemplo

- Vou usar o **algoritmo de Grover** — algoritmo quântico que busca numa base de dados não ordenada — como exemplo. Temos um ficheiro com 1.000.000 de linhas e queremos encontrar a única que satisfaça uma dada condição. Em computação clássica, um roteiro em **bash** faria inevitavelmente qualquer coisa como:

```
while IFS= read -r linha; do
    if condicao "$linha"; then
        echo "$linha"
        break
    fi
done < base_de_dados.txt
```

- No pior caso, leria todas as linhas até achar a certa: N passos. Contudo, em média leria N/2. É uma busca linear, inevitável classicamente sem ordenação prévia.

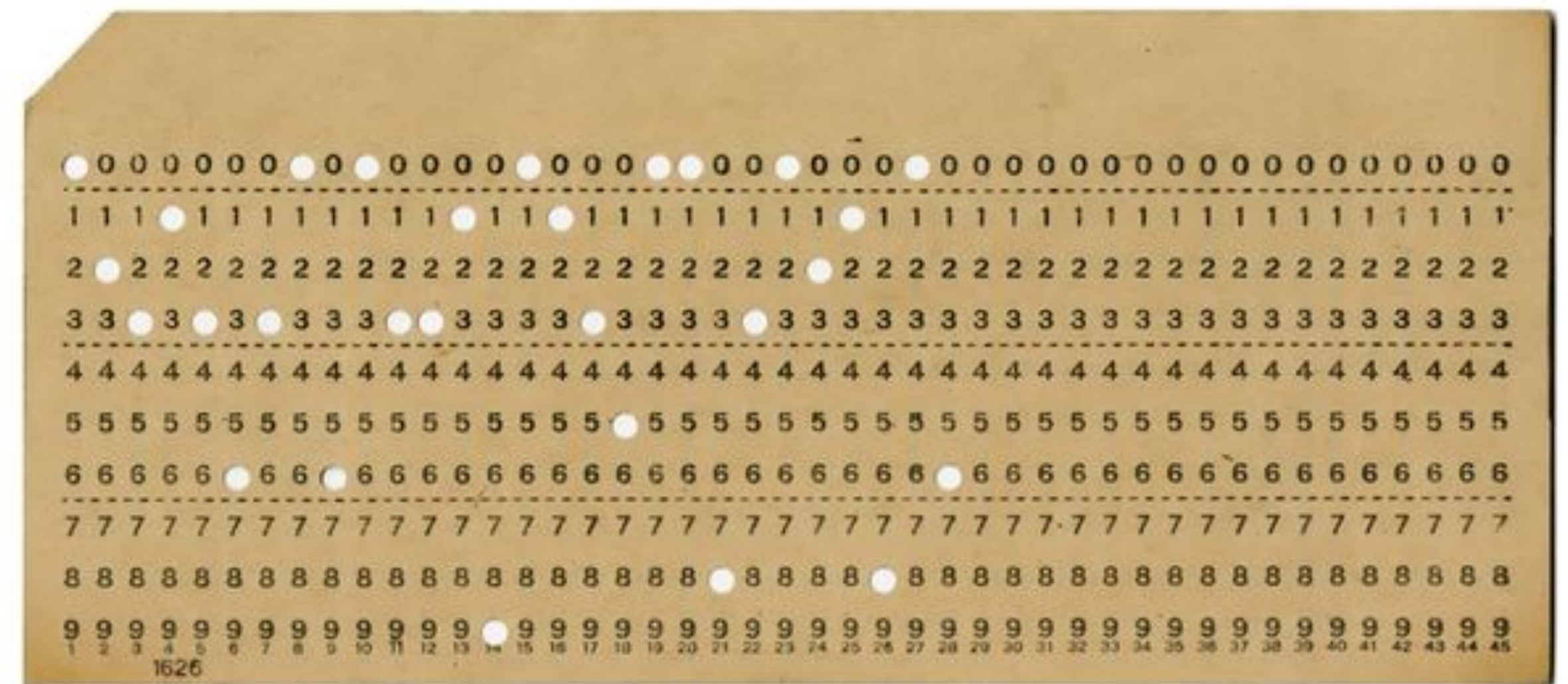
para comparação com o meu exemplo...

```
60 ~
61 # Pré-carregar as assinaturas existentes~
62 declare -A CHECKSUMS_EXISTENTES~
63 declare -A VISTOS...# ficheiros realmente processados nesta corrida~
64 ~
65 # Nota: guardamos URLs exactamente como aparecem no ficheiro (incluindo espaços)~
66 # porque o formato é "MD5<espaço>URL" ~
67 while IFS= read -r LINE || [[ -n "$LINE" ]]; do~
68     ... MD5="${LINE%*}"~
69     ... FICHEIRO="${LINE#*}"~
70     ... [[ -n "$MD5" && -n "$FICHEIRO" ]] && CHECKSUMS_EXISTENTES["$FICHEIRO"]="$MD5"~
71 done < "$CHECKSUM_FILE"~
72 ~
73 while IFS= read -d ' ' -r FICHEIRO; do~
74     ...# Marcar como visto nesta corrida~
75     ... VISTOS["$FICHEIRO"]=1~
76 ~
77     ...# Processar ficheiros FLAC~
78     ... if [[ "$FICHEIRO" == *.flac ]]; then~
79         ... MD5_ATUAL=$( /usr/local/bin/metaflac --show-md5sum "$FICHEIRO" )~
80 ~
81         ... if ! /usr/local/bin/flac -s --threads="$NUM_THREADS" --test "$FICHEIRO"; then~
82             ... echo "🔴 Falha de integridade: '$FICHEIRO' corrompido!"~
83             ... ((CORROMPIDOS++))~
84             ... continue~
85         ... fi~
86 ~
87 ~
88 ~
89 ~
90 ~
91 ~
92 ~
93 ~
94 ~
95 ~
96 ~
97 ~
98 ~
99 ~
100 ~
```


Métodos antigos de programação e de inserção de dados: cartões perfurados



tear Jacquard



computador

- **O equivalente quântico:**

- O algoritmo de Grover faz o mesmo em $\sim\sqrt{N}$ passos. Para 1.000.000 de entradas, passará de 500.000 passos em média média para ~ 1.000 .
- O mecanismo por trás disto não é «ver tudo ao mesmo tempo» (isto é um equívoco comum acerca de computação quântica). O que acontece é:
 1. O registo de qubits é preparado em superposição de todos os estados possíveis.
 2. Um operador (o **oráculo**) inverte a fase do estado que satisfaz a condição, sem o identificar explicitamente;
 3. Um segundo operador amplifica iterativamente a amplitude de probabilidade desse estado à custa da amplitude dos outros estados.
 4. Após $\sim\sqrt{N}$ iterações, uma medição encontra a solução com probabilidade elevada.

- A analogia **bash** seria um script que, em vez de testar as linhas sequencialmente, conseguisse a cada iteração tornar a linha correcta *mais provável* e todas as outras *menos prováveis* — até que ao fim de $\sqrt{N}$ iterações bastasse ler uma única linha.
- O ponto crucial: o ganho não vem de paralelismo bruto, mas de interferência construtiva e destrutiva entre amplitudes — **que é uma propriedade ondulatória sem equivalente clássico.**

1. Superposição de todos os estados

- No computador, uma variável **bash** tem um valor de cada vez — por exemplo $x=3$. Um qubit pode estar num estado que é, de certa forma, uma combinação de 0 e 1 simultaneamente — não porque «seja os dois», mas porque a sua evolução futura carrega informação sobre ambos.
- Com N qubits, o sistema descreve-se como uma combinação de todos os 2^N estados possíveis ao mesmo tempo. Para 20 qubits, são mais de um milhão de estados — todos presentes **simultaneamente** na descrição matemática do sistema.

2. O oráculo inverte a fase do estado correcto

- *Fase* aqui é a fase de uma onda — o mesmo conceito das ondas electromagnéticas que já discutimos. Cada estado na superposição tem uma amplitude complexa, com módulo e fase. O oráculo é uma operação que muda o sinal da amplitude do estado que satisfaz a condição (de $+a$ para $-a$) sem alterar mais nada. Matematicamente é simples; fisicamente é subtil porque o sistema **ainda não sabe** qual é a resposta.

Qual é a estrutura física do oráculo?

É uma sequência de portas quânticas

- **Portas clássicas vs. portas quânticas:**

- Uma porta AND, OR ou NOT clássica é um dispositivo físico (um transístor, essencialmente) que transforma bits de entrada em bits de saída. Uma porta quântica é uma operação unitária: uma rotação no espaço de estados do qubit, que transforma amplitudes.
- As portas quânticas elementares têm nomes como X, H, CNOT, Toffoli. A porta H (Hadamard) é a que cria superposição a partir de um estado definido e a que teríamos usado no algoritmo de Grover. A CNOT inverte um qubit condicionalmente ao estado de outro e é a base do emaranhamento entre qubits.
- O oráculo, concretamente, é uma sequência específica destas portas, disposta de forma a implementar a função:
 - a. se o estado de entrada satisfaz a condição $\rightarrow$ inverte a fase
 - b. caso contrário $\rightarrow$ não faz nada

3. Amplificação por interferência

- Aqui está o cerne. Aplica-se depois um operador que usa interferência (como duas ondas que se somam ou que se cancelam) para aumentar a amplitude do estado com fase invertida e diminuir todas as outras. É destrutivo para os estados errados, construtivo para o correcto. Cada iteração aumenta a probabilidade do estado correcto: o estado-resposta.

4. Medição

- Após $\sqrt{N}$ iterações, o estado correcto tem amplitude dominante. Ao medir, isto é, ao *ler* o sistema, obtém-se esse estado com probabilidade muito elevada. A medição em mecânica quântica colapsa a superposição num único resultado.
- A analogia **bash** completa seria esta: imagina que a base de dados de um milhão de linhas fosse uma onda, e que cada linha tivesse uma amplitude. O roteiro *afinaria* essa onda iterativamente, como se ajustasses interferências, até a linha correcta *ressoar* e todas as outras se cancelarem. Ao fim de ~ 1000 afinações, bastaria uma leitura para se ter a resposta.

Entrada de informação nos sistema clássico vs. quântico

- **Num computador clássico moderno:**
 - Carregam-se os dados para memória: o ficheiro com a base de dados é lido, os valores ficam em RAM, o processador acede-lhes por endereço de memória. É um processo físico directo e intuitivo.
- **Num computador quântico:**
 - Não há *carregamento de dados* no mesmo sentido. O que existe é a codificação do problema na própria estrutura do oráculo e este é o ponto menos intuitivo de toda a computação quântica.
 - O oráculo não é um ficheiro que o computador lê. É uma operação unitária; uma transformação física do sistema de qubits, construída especificamente para o problema em questão. A informação está incorporada na própria operação, não num espaço de memória separado.
 - Uma analogia imperfeita mas útil: em vez de se escrever os dados num ficheiro e se mandar um roteiro processá-los, imaginemos que se construía um circuito físico diferente para cada problema e que a estrutura de circuito era os dados.

ASICs

- Um ASIC (*Application-Specific Integrated Circuit*), como o *Jalapeño* para bitcoin que mencionei, é um circuito de computação construído para um problema específico: a sua arquitectura é o algoritmo, ao contrário de um processador de uso geral (CPU) que executa instruções arbitrárias. O ASIC sacrifica polivalência em favor de eficiência máxima num domínio restrito.
- Um computador quântico actual partilha exactamente essa característica: o problema está em grande medida incorporado na construção do circuito quântico, na sequência de portas e estrutura do oráculo, e não num programa a correr no hardware.
- Contudo, enquanto os ASICs são completamente fixos após fabrico, os circuitos quânticos actuais são reconfiguráveis e é possível programar sequências diferentes de portas sobre o mesmo hardware físico. Nesse sentido estão algures entre um ASIC e um FPGA (*Field-Programmable Gate Array*) — hardware reconfigurável mas com uma arquitectura base fixa para um dado problema.
- Outra diferença é que nos ASICs a especialização é uma **escolha** de engenharia para ganhar desempenho. Nos computadores quânticos actuais é uma **limitação** intrínseca: ainda não existe um modelo verdadeiramente de uso geral com vantagem quântica demonstrada em problemas práticos amplos.
- Mas como intuição de que *a informação está na estrutura do circuito e não num ficheiro de dados separado*, a analogia com os ASICs é das melhores que se pode fazer com conceitos clássicos.

Qubits

- Um *qubit* (abreviatura de *quantum bit*) é a unidade fundamental de informação em computação quântica, análoga ao bit clássico. Enquanto um bit clássico só pode assumir o valor 0 ou 1, um qubit pode existir numa **superposição** desses dois estados em simultâneo, ou seja, é parcialmente 0 e parcialmente 1, com amplitudes de probabilidade associadas a cada um dos estados. Só no momento da medição o estado **colapsará** para um valor definido de 0 ou 1.

- Formalmente, o estado de um qubit escreve-se:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- onde α e β são números complexos (as amplitudes) que satisfaçam

$$|\alpha|^2 + |\beta|^2 = 1$$

- Para além da superposição, os qubits podem estar **emaranhados** (*entangled*) com outros qubits, de modo que o estado de um não pode ser descrito independentemente do outro (esta propriedade não tem equivalente clássico e é essencial para a vantagem computacional quântica).
- Fisicamente, um qubit pode ser implementado como iões aprisionados, circuitos supercondutores, centros de cor em diamantes ou a polarização de um fóton.

Emaranhamento Quântico

Emaranhamento Quântico

Ponto de partida

- O emaranhamento parece misterioso
- Mas os conceitos básicos podem ser entendidos de forma simples
- Depois de entendidos preparam-nos para perceber os «muitos mundos» da teoria quântica

Sistemas c-ons

Considere-se...

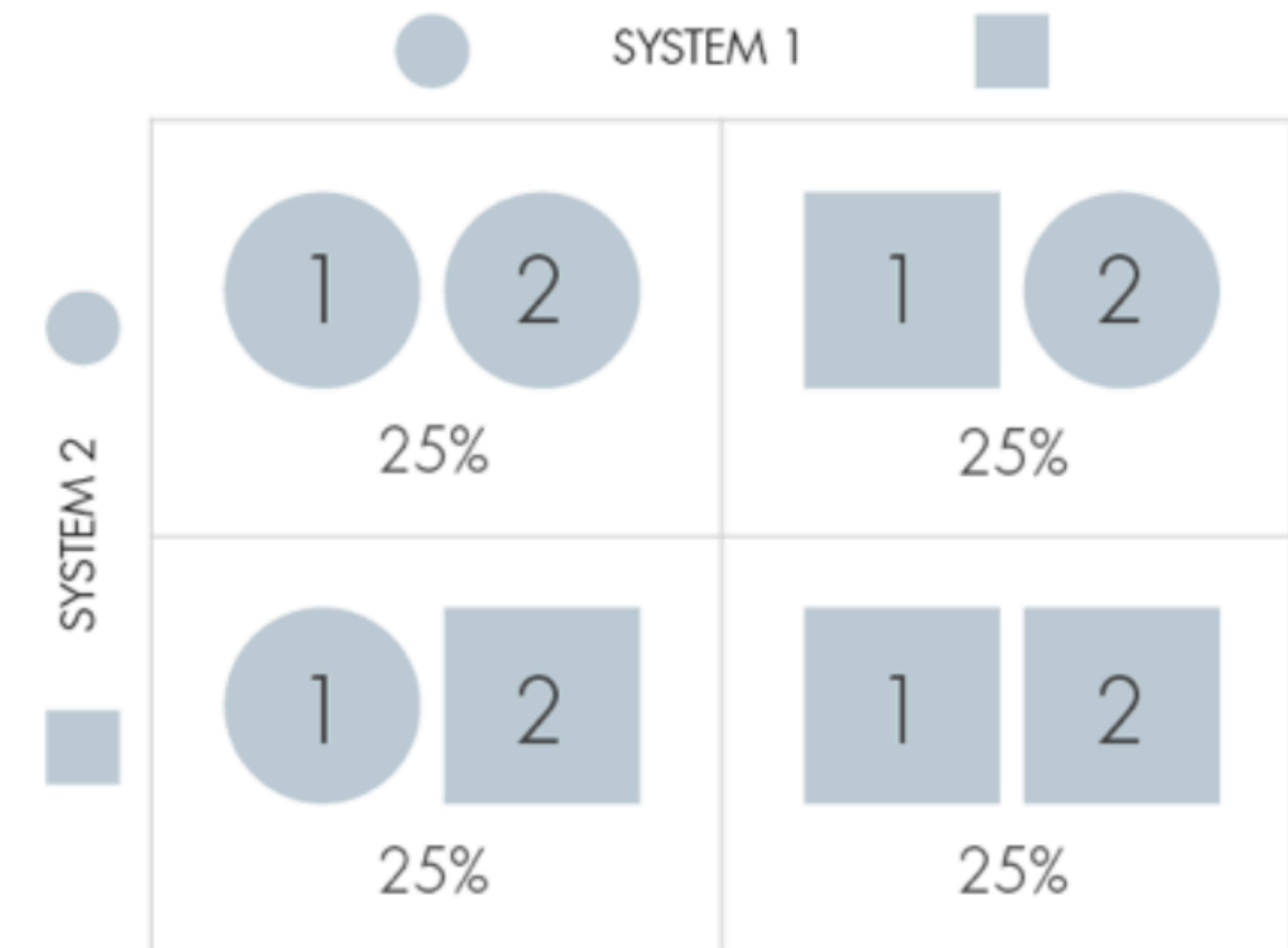
- O **emaranhamento** ocorre quando temos conhecimento parcial do estado de dois sistemas. Por exemplo, o nosso sistema poderá ser dois objectos que chamaremos c-ons. Estes dois objectos apresentam duas formas: quadrados ou círculos que identificamos como os seus estados possíveis.
- Haverá então 4 estados possíveis para dois c-ons: (square, square), (square, circle), (circle, square), (circle, circle).
- Podemos de seguida definir as probabilidades de encontrar o sistema em cada um destes quatro estados.

Independência

Conhecer um estado não informa o outro

- Dizemos que os c-ons são independentes se o conhecimento do estado de um não informa acerca do estado do outro. Se soubermos que um é um quadrado, continuaremos sem saber qual será a forma do segundo. E vice-versa, se soubermos a forma do segundo, não saberemos a do primeiro.
- Os estados tem **probabilidades separadas**

INDEPENDENT

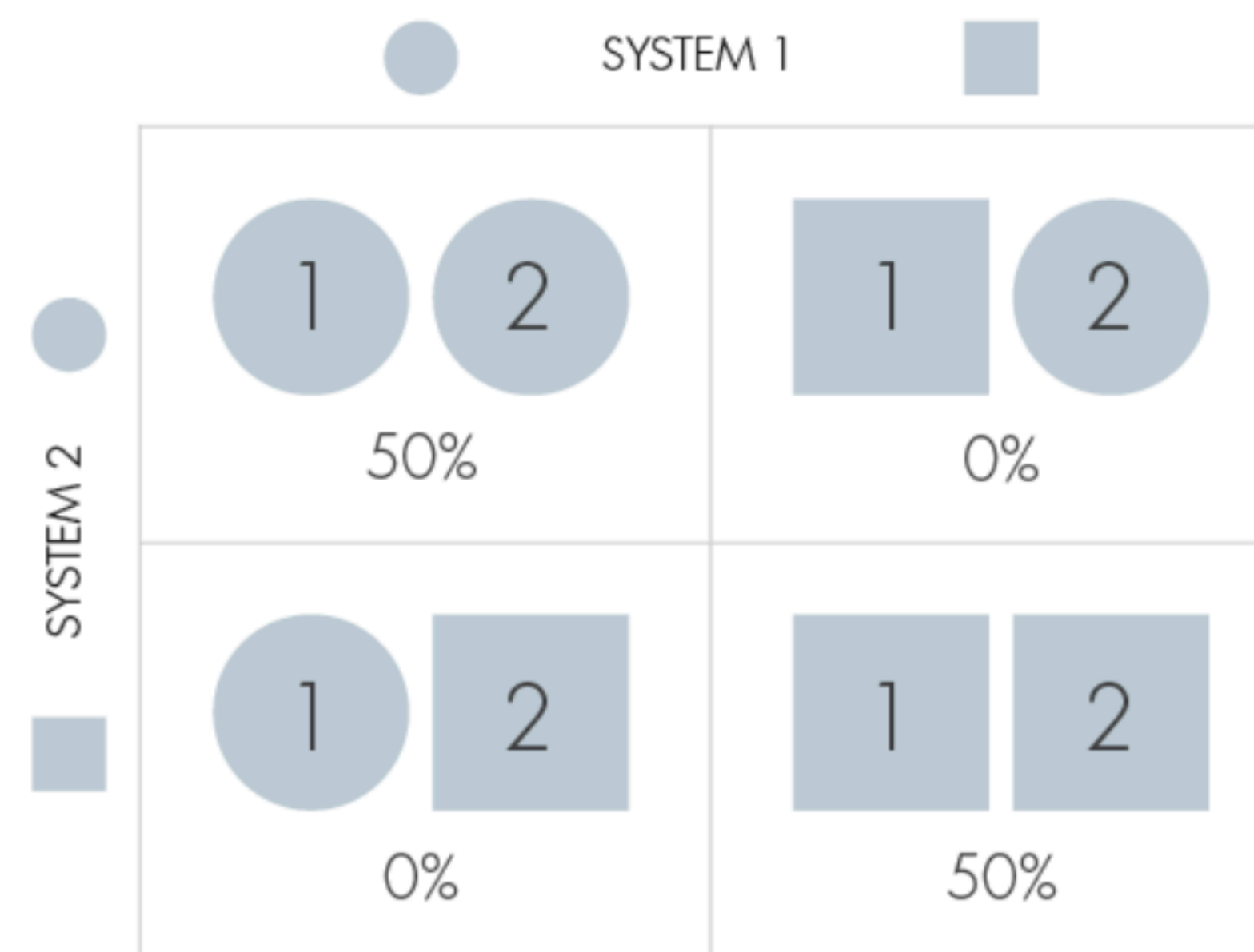


Emaranhamento clássico

Correlação total

- Por outro lado, dizemos que os c-ons estão emaranhados quando a informação acerca de um, melhora o nosso conhecimento do outro. No caso do emaranhamento extremo mostrado aqui, quando o primeiro c-on é circular, sabemos que o segundo também será circular. E quando o primeiro é um quadrado, o segundo também o será.
- Sabendo a forma de um, permite-nos inferir com muita certeza a forma do outro.

ENTANGLED



Ideia essencial

Emaranhamento e independência

- A versão quântica de emaranhamento é essencialmente o mesmo fenómeno. Isto é, falta de independência. Em teoria quântica, os estados são descritos por objectos matemáticos chamados funções de onda. As regras que ligam funções de onda às probabilidades físicas introduzem complicações interessantes, mas o conceito central de emaranhamento continua a poder ser aplicado.
- Formas não contam como sistemas quânticos, mas conseguimos partículas emaranhadas nas situações que descrevemos anteriormente. Nomeadamente, poderemos obtê-las após a colisão de partículas. Verdade seja dita, estados não-emaranhados (independentes) são excepções raras, pois quando os estados interagem, a interacção cria correlações entre eles.
- Por exemplo, as moléculas são compósitos de subsistemas, nomeadamente de electrões e de núcleos. A molécula no seu estado de energia mais baixo, no qual geralmente está, é um estado muito emaranhado dos seus electrões e núcleos, pois a sua posição não é de forma alguma independente. O movimento do núcleo é acompanhado pelo movimento em simultâneo dos electrões.
- O emaranhamento é assim *a falta de independência*.

Passagem ao quântico

Funções de onda

- Estados $\rightarrow$ funções de onda
- Independentes: $\Phi_{\blacksquare}\Psi_{\blacksquare} + \Phi_{\blacksquare}\Psi_{\bullet} + \Phi_{\bullet}\Psi_{\blacksquare} + \Phi_{\bullet}\Psi_{\bullet}$
- Emaranhadas: $\Phi_{\blacksquare}\Psi_{\blacksquare} + \Phi_{\bullet}\Psi_{\bullet}$ ou $(\Phi_{\blacksquare} + \Phi_{\bullet})(\Psi_{\blacksquare} + \Psi_{\bullet})$
- É de notar como esta última formulação separa claramente o sistema 1 e o sistema 2 em unidades independentes.

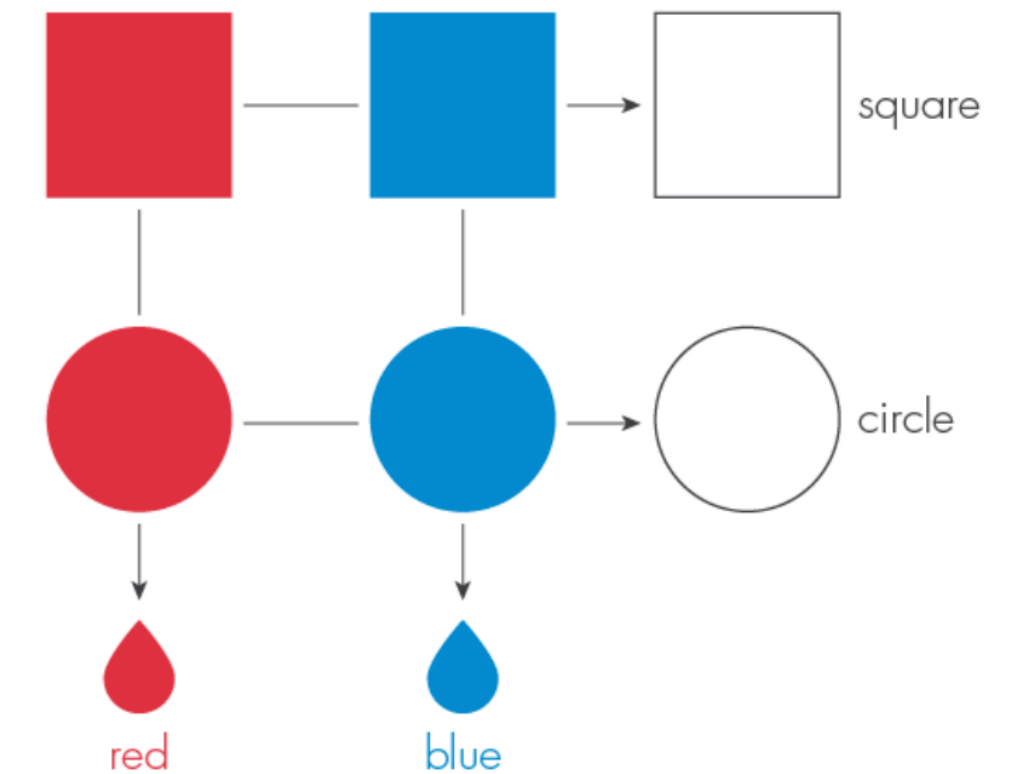
Nota

- Há muitas formas de criar estados emaranhados. Uma forma seria a de medir o nosso sistema compósito de forma a obter informação parcial. Por exemplo, poderíamos saber que os dois sistemas tem a mesma forma mas sem sabermos que forma têm. Este conceito será importante mais adiante.

Complementaridade

- As consequências mais marcantes do emaranhamento quântico como os efeitos Einstein-Podolsky-Rosen (EPR) e Greenberger-Horne-Zeilinger (GHZ) surgem com a interacção do emaranhamento com outro aspecto da teoria quântica chamado **complementaridade**. Para preparar a discussão de EPR e de GHZ falemos um pouco de complementaridade.

Consequências



- Anteriormente, imaginávamos que os c-ons poderiam ter duas formas (quadrados e círculos). Agora imaginemos que poderão também ter duas cores: vermelho e azul.
- Se falarmos de sistemas clássicos, esta propriedade adicional implicará que os nossos c-ons possam estar num de quatro estados possíveis: quadrado vermelho, círculo vermelho, quadrado azul ou círculo azul.
- Contudo num sistema quântico, a q-on a situação será profundamente diferente. O facto de que um *q-on* possa exhibir em condições diferentes formas diferentes e cores diferentes, não quer dizer que possua forma e cor simultaneamente. Esta intuição de senso-comum é incompatível com a realidade experimental: podemos medir a forma do nosso q-on, mas ao fazermos isso perdemos a informação acerca de sua cor. Ou podemos medir a cor do nosso q-on, mas ao fazemos isso **perdemos toda a informação acerca de sua forma**.

- De acordo com a teoria quântica o que não conseguimos fazer é simultaneamente medirmos a forma e a cor simultaneamente. Nenhuma vista única da realidade capturará todos os seus aspectos. Teremos que considerar muitas vistas diferentes e mutuamente exclusivas, cada uma das quais a oferecer informação válida mas parcial. Isto é o cerne da *complementaridade* como Niels Bohr a formulou.
- Uma consequência é que a teoria quântica nos força a ser cautelosos na forma como atribuímos realidade física a propriedades individuais.
- Para evitar contradições teremos que pressupor:
 1. Uma propriedade que não for medida não terá que existir.
 2. A medição é um processo activo que *altera* o sistema medido.

Falaremos agora de duas ilustrações da peculiaridade da teoria quântica. Ambas foram testadas experimentalmente de forma rigorosa.

**Albert Einstein, Boris Podolsky e
Nathan Rosen (efeito EPR)**

- Um par EPR consiste em dois q-ons, cada um dos quais poderá ser medido por sua forma ou por sua cor, mas não por ambas.
- Nós pressupomos que temos acesso a muitos desses pares, todos idênticos, e que podemos escolher que medições fazer de seus componentes.
- Se medirmos a forma de um dos membros de um par EPR, veremos que há uma probabilidade igual de ser um quadrado ou um círculo. Se medirmos cor, de ser vermelho ou azul.
- O efeito interessante, considerado paradoxal por EPR, surge quando se medem ambos os membros de um par. Se medirmos ambos para cor ou para forma, os resultados *coincidirão* sempre. Assim, se medirmos que um é vermelho e mais tarde medirmos o outro, o outro também será vermelho. Contudo, se medirmos a cor de um e mais tarde a forma do outro, veremos que não há correlação. Assim, se a forma do primeiro for um quadrado, o segundo terá igual probabilidade de ser vermelho ou de ser azul.

- De acordo com a teoria quântica, obteremos esses resultados mesmo que grandes distâncias separem os dois sistemas e as medições sejam realizadas quase simultaneamente. A escolha da medição numa localização parece estar a afetar o estado do sistema na outra localização.
- Este «efeito remoto assustador» (*spukhafte Fernwirkung*), como lhe chamou Einstein, poderia parecer exigir a transmissão de informação — neste caso, informação sobre qual medição foi realizada — a uma velocidade superior à da luz. Mas será que exige mesmo?
- Enquanto não conhecer o resultado obtido, não sei o que esperar. Obtenho informação útil quando conheço o resultado medido, não no momento em que foi medido. E qualquer mensagem que me revele o resultado medido tem que ser transmitida de forma física concreta, mais lentamente (presumivelmente) do que a da luz.

- Ao refletir mais profundamente, o paradoxo dissolve-se ainda mais. Com efeito, consideremos novamente o estado do segundo sistema, dado que o primeiro foi medido como vermelho. Se escolhermos medir a cor do segundo q-on, obteremos certamente vermelho. Mas, como discutimos anteriormente, ao introduzir a complementaridade, se escolhermos medir a forma de um q-on, quando este está no estado «vermelho», teremos igual probabilidade de encontrar um quadrado ou um círculo. Assim, longe de introduzir um paradoxo, o resultado EPR é logicamente forçado. É, em essência, simplesmente uma reconfiguração da complementaridade.
- Também não será paradoxal descobrir que eventos distantes estão correlacionados. Afinal, se colocar cada elemento de um par de luvas em caixas e as enviar para lados opostos da Terra, não deveria ficar surpreendido por, ao olhar dentro de uma caixa, poder determinar a que mão pertence a luva na outra.
- Da mesma forma, em todos os casos conhecidos, as correlações entre um par EPR devem ser impressas quando os seus membros estão próximos, embora possam, obviamente, sobreviver à separação subsequente, como se tivessem memórias. Outra vez: a peculiaridade do EPR não é a correlação em si, **mas a sua presença física nas formas complementares.**

**Daniel Greenberger, Michael
Horne e Anton Zeilinger (o estado
GHZ)**

- Daniel Greenberger, Michael Horne e Anton Zeilinger descobriram outro exemplo extraordinariamente elucidativo do entrelaçamento quântico. Envolve três dos nossos q-ons, preparados num estado especial e entrelaçado (o estado GHZ).
- Distribuámos os três q-ons por três experimentadores distantes. Cada experimentador escolhe, de forma independente e aleatória, se mede a forma ou a cor, e regista o resultado.
- A experiência é repetida muitas vezes, começando sempre os três q-ons no estado GHZ. Cada experimentador, individualmente, obtém resultados maximamente aleatórios. Quando mede a forma de um q-on, tem igual probabilidade de encontrar um quadrado ou um círculo; quando mede a sua cor, vermelho ou azul são igualmente prováveis. Até aqui, tudo bastante corriqueiro.

- Contudo, quando mais tarde os experimentadores se reúnem e comparam as suas medições, a análise de dados revela um resultado impressionante!
- Para percebermos melhor o efeito e este resultado, agrupemos os resultados possíveis. Assim, chamemos «bom» à forma quadrado e à cor vermelho e «mau» à forma círculo e à cor azul.
- Os experimentadores descobrem que, sempre que dois deles mediram a forma e o terceiro mediu a cor, obtiveram exatamente 0 ou 2 resultados «maus» (isto é, círculos ou azul). Mas quando todos os três escolheram medir a cor, obtiveram exatamente 1 ou 3 resultados «maus».
- Isto é o que a mecânica quântica prevê, e é o que se observa. Então: a quantidade de «mau» é par ou ímpar? Como ambas as possibilidades se realizam, com certeza, em diferentes tipos de medições, somos forçados a rejeitar a pergunta. Não faz sentido falar da quantidade de «mau» no nosso sistema, independentemente de como é medida. Com efeito, isso leva a contradições.

- O efeito GHZ é, nas palavras do físico Sidney Coleman, «um soco de mecânica quântica no nariz do leitor». Este efeito destrói um preconceito profundamente enraizado, baseado na experiência quotidiana, de que os sistemas físicos têm propriedades definidas, independentemente dessas propriedades serem ou não medidas. Pois se assim fosse, o equilíbrio entre «bom» e «mau» não seria afetado pelas escolhas de medição.
- Uma vez interiorizada, a mensagem do efeito GHZ é inesquecível e expande a mente.

