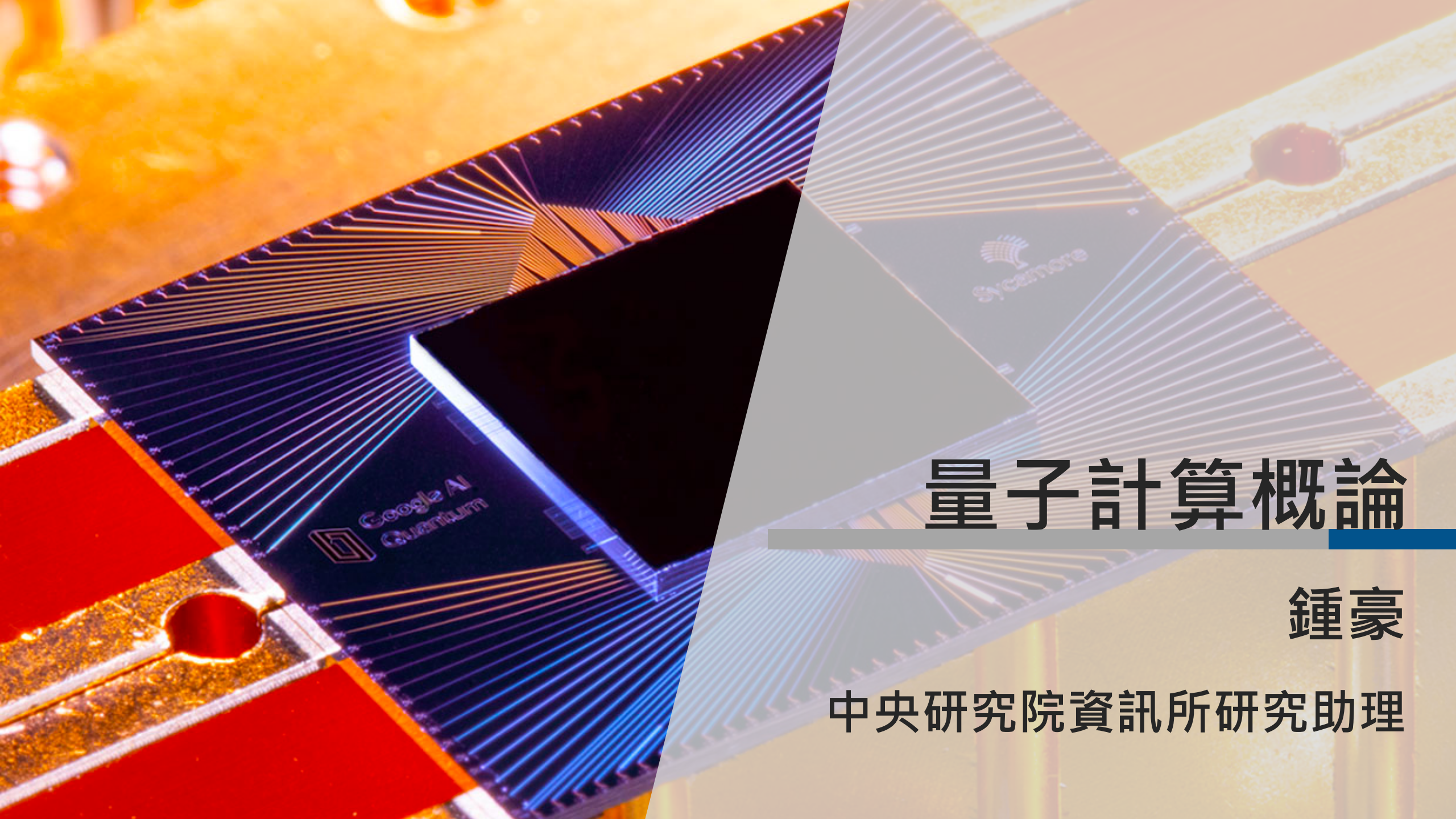


量子計算概論

鍾豪

中央研究院資訊所研究助理

講者介紹 Speaker

現職：中研院資訊所研究助理

- 研究領域：區塊鏈、量子密碼

學歷：台大物理學士、台大電機碩士

27 Sep 2019 | 17:35 GMT

Google 做了什麼事？

什麼是量子霸權？

What Google's Quantum Supremacy Claim Means for Quantum Computing

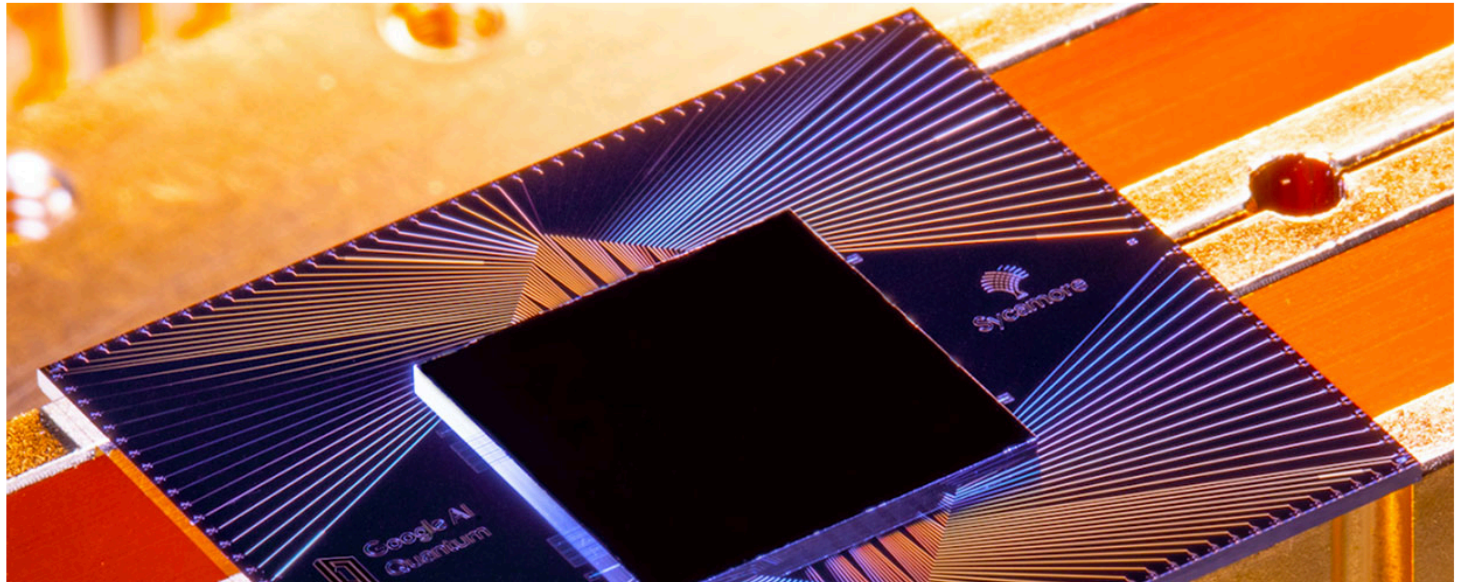
什麼是量子計算？

Leaked details about Google's quantum supremacy experiment stirred up a media frenzy about the next quantum computing milestone

量子電腦能做什麼事？

By **Jeremy Hsu**

我們的網際網路還是安全的嗎？



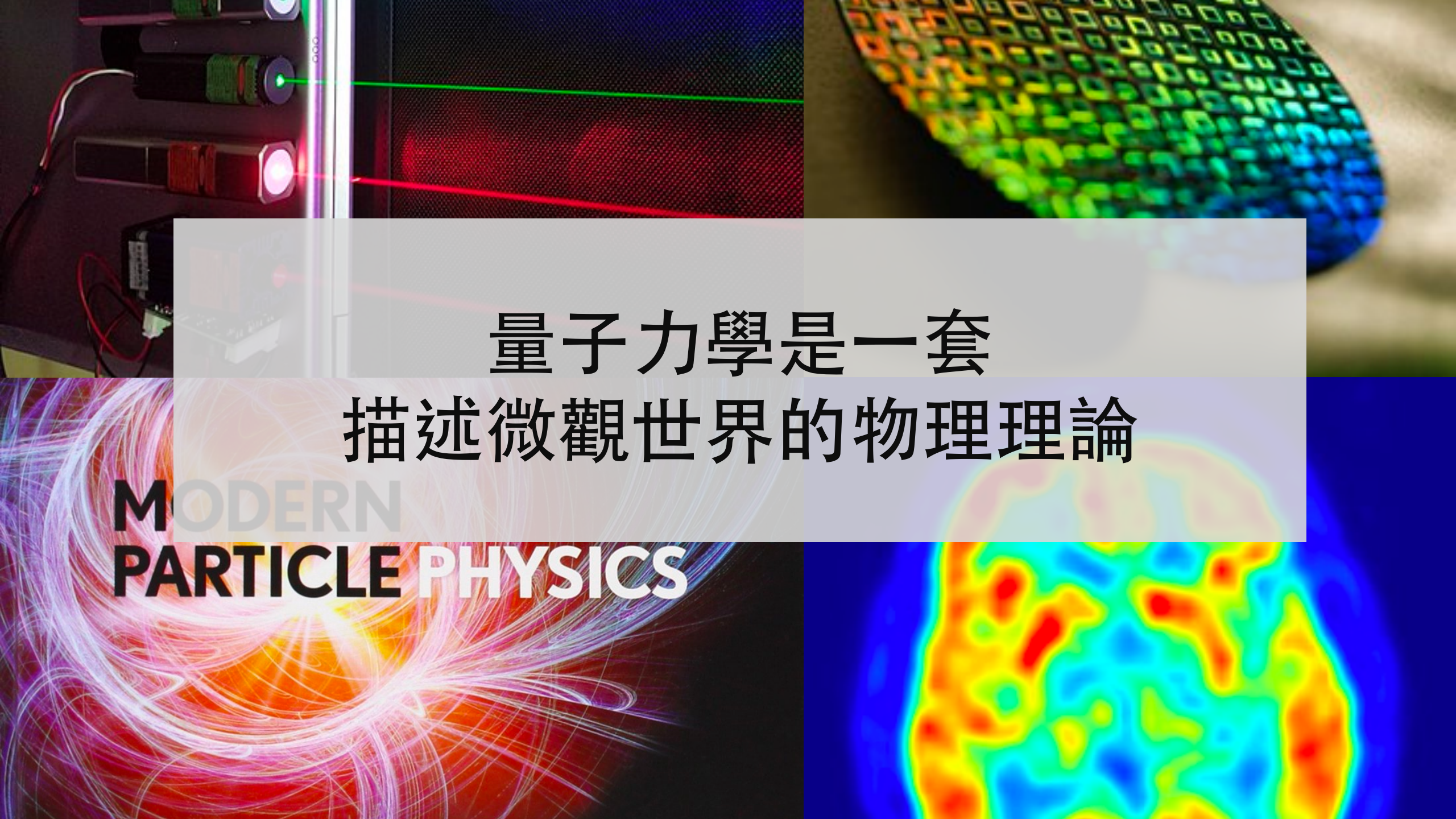
大綱 Outline

1. 什麼是量子？
2. 量子系統的威力與代價：疊加與糾纏
   - 量子電腦的優勢：模擬量子系統
   - 量子電腦的優勢：量子演算法
3. 量子電腦的迷思

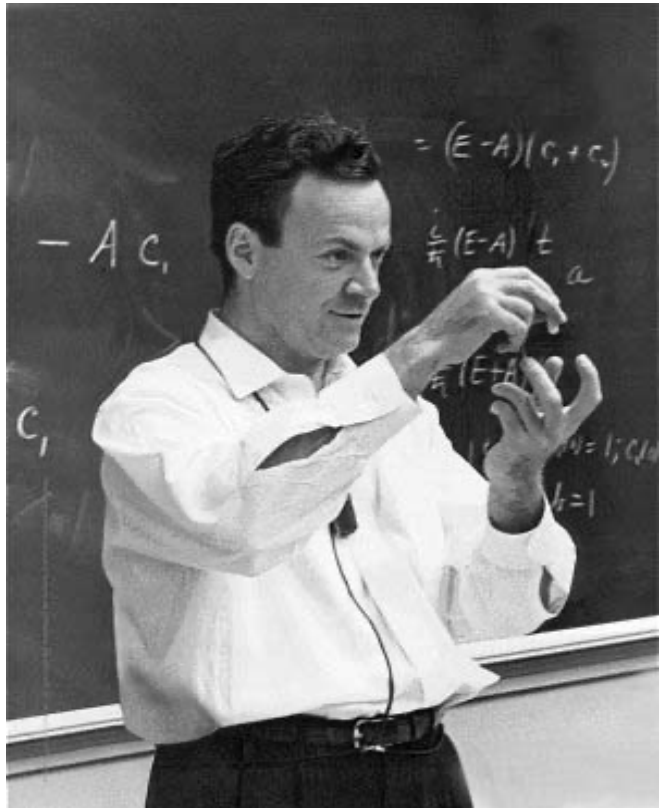
What is QUANTUM?

Max Planck (1858-1947)

$$E = nh\nu$$



量子力學是一套
描述微觀世界的物理理論



Richard Feynman (1918-1988)
於1982年首度提出量子電腦的構想

therefore, the problem is, how can we simulate the quantum mechanics? There are two ways that we can go about it. We can give up on our rule about what the computer was, we can say: Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws. Or

概念上是讓電腦本身具有量子的特性

大綱 Outline

1. 什麼是量子？
2. 量子系統的威力與代價：疊加與糾纏
   - 量子電腦的優勢：模擬量子系統
   - 量子電腦的優勢：量子演算法
3. 量子電腦的迷思

符號 Notation

在量子計算中，我們會使用狄拉克記號“ $|\cdot\rangle$ ”來代表一個系統的「狀態」

比方說，一個銅板的狀態可能為

$$|\text{正面}\rangle \text{ 或 } |\text{反面}\rangle.$$

又或者，一顆骰子的狀態可能為

$$|1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle \text{ 或 } |6\rangle.$$

一個**量子位元 (qubit)** 就是任何具有兩種狀態的量子系統，通常寫為

$$|0\rangle \text{ 或 } |1\rangle.$$

Superposition

古典銅板 Classical Coin

一個古典銅板當下的狀態只能是
「正面」或是「反面」其中一種

$\frac{1}{2}$: Tail

$\frac{1}{2}$: Head

量子銅板 Quantum Coin

一個量子銅板當下的狀態可以
「同時」處於正面及反面的疊加態

$$\frac{1}{\sqrt{2}}|\text{Head}\rangle + \frac{1}{\sqrt{2}}|\text{Tail}\rangle$$

疊加 Superposition

一個古典位元只能是「0」或是「1」

一個量子位元 (qubit) 可以處於「0」與「1」的疊加態

$$\alpha|0\rangle + \beta|1\rangle.$$

當我們測量時，會以$|\alpha|^2$的機率得到「0」，以$|\beta|^2$的機率得到「1」

- 由於機率和必為1，所以α與β有以下關係

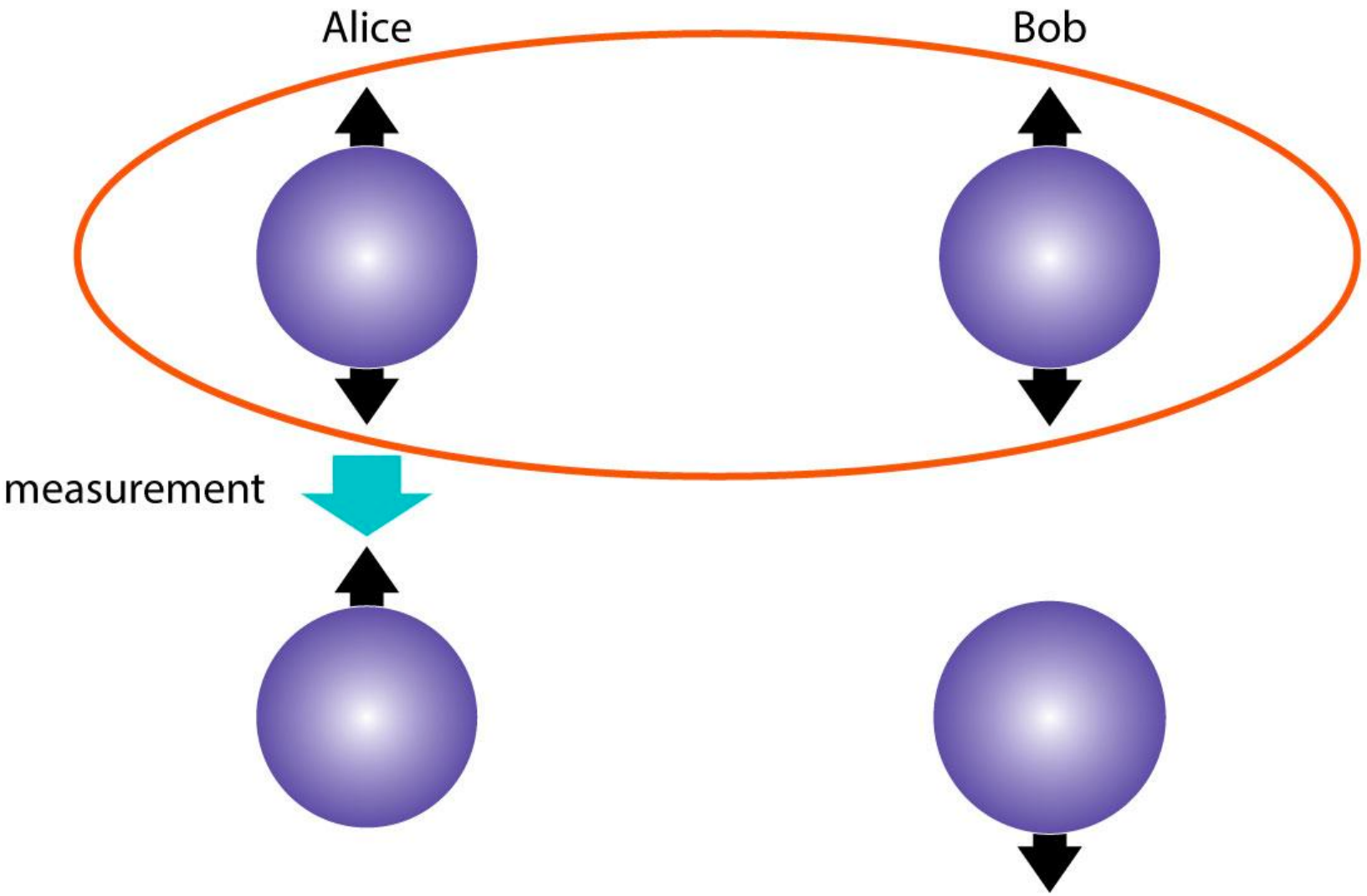
$$|\alpha|^2 + |\beta|^2 = 1.$$

對於一個量子位元，我們需要兩個數字 (α, β) 來描述

假設我們有 20 個量子位元，那麼需要幾個數字才能描述呢？

Entanglement

糾纏 Entanglement



糾纏 Entanglement

由於量子系統有可能互相糾纏的關係，我們必須將整個系統視為一個整體

因此，要描述一個「三個 qubits」的系統，其量子態為

$$a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle$$

我們需要 8 個數字才能描述「三個 qubits」的系統，而非 $2\times3 = 6$ 個數字

因此，當量子系統規模大時，古典電腦就難以儲存且運算該系統

量子電腦優勢：模擬量子系統

要描述一個 n 量子位元的量子系統，需要 2^n 個係數

但是，量子電腦並非在這些係數上運算，而是將量子位元直接設定成系統的量子態，並指定計算 (演化) 過程

因此，要模擬一個 n 量子位元的量子系統，邏輯上只需要 n 個量子位元

量子電腦優勢：量子平行計算

$$|x\rangle \rightarrow \boxed{f} \rightarrow |f(x)\rangle$$

如果我們有個 n 量子位元的系統，並將初始狀態設為 $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$

則運算完後，我們可以得到

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|f(x)\rangle$$

2^n個函數值在疊加態中，
被一口氣運算出來

量子電腦優勢：量子平行計算

假設 $f(x) = 3x + 1$，且設定初始狀態為

$$|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

則經過量子運算後，我們可得

$$|\psi'\rangle = \frac{1}{2}(|0\rangle + |4\rangle + |7\rangle + |10\rangle)$$

但是，測量時只能得到其中一種狀態
問題在於，要如何取得我們有興趣的答案？

量子電腦優勢：量子平行計算

「量子平行」是利用疊加的特性，
達到一次操作即可同時計算多個疊加態

大多數量子演算法的設計巧妙在於
「如何操控係數，使我們測量到需要的結果」

Fields of Application

Cryptography 破密

- Quantum computers have the potential to keep private data safe from snoops and hackers, no matter where it is stored or processed.

Medicine & Materials 製藥、材料化學

- A quantum computer mimics the computing style of nature, allowing it to simulate, understand and improve upon natural things—like molecules, and their interactions.

Machine Learning 機器學習演算法

- Research indicates that quantum computing could significantly accelerate machine learning and data analysis tasks.

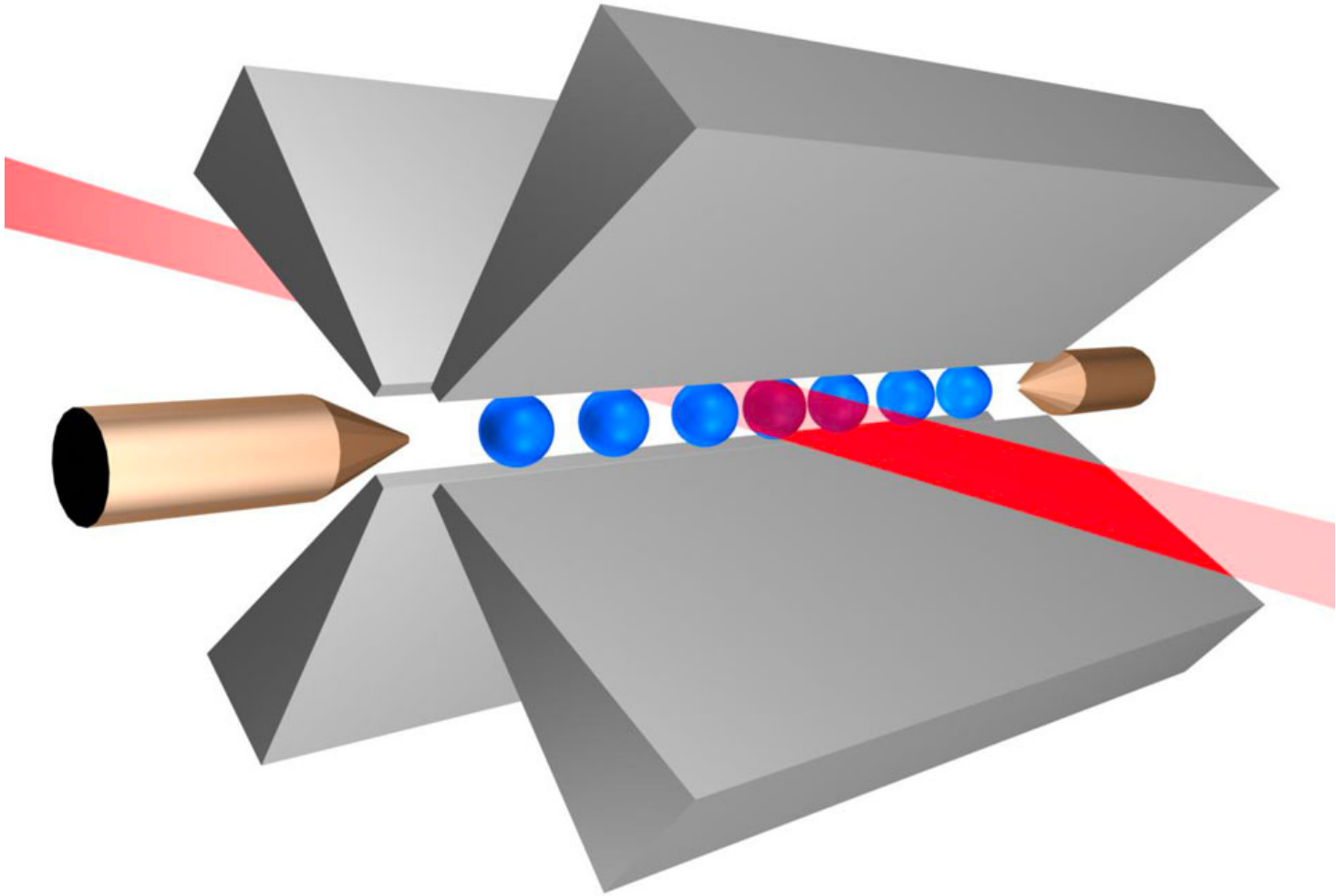
Searching Big Data 搜尋問題

- Quantum computing can search the ever-growing amount of data being created, and locate connections within it, significantly faster than classical computers, that will have tremendous impact across many industries.

大綱 Outline

1. 什麼是量子？
2. 量子系統的威力與代價：疊加與糾纏
   - 量子電腦的優勢：模擬量子系統
   - 量子電腦的優勢：量子演算法
3. 量子電腦的迷思

離子阱



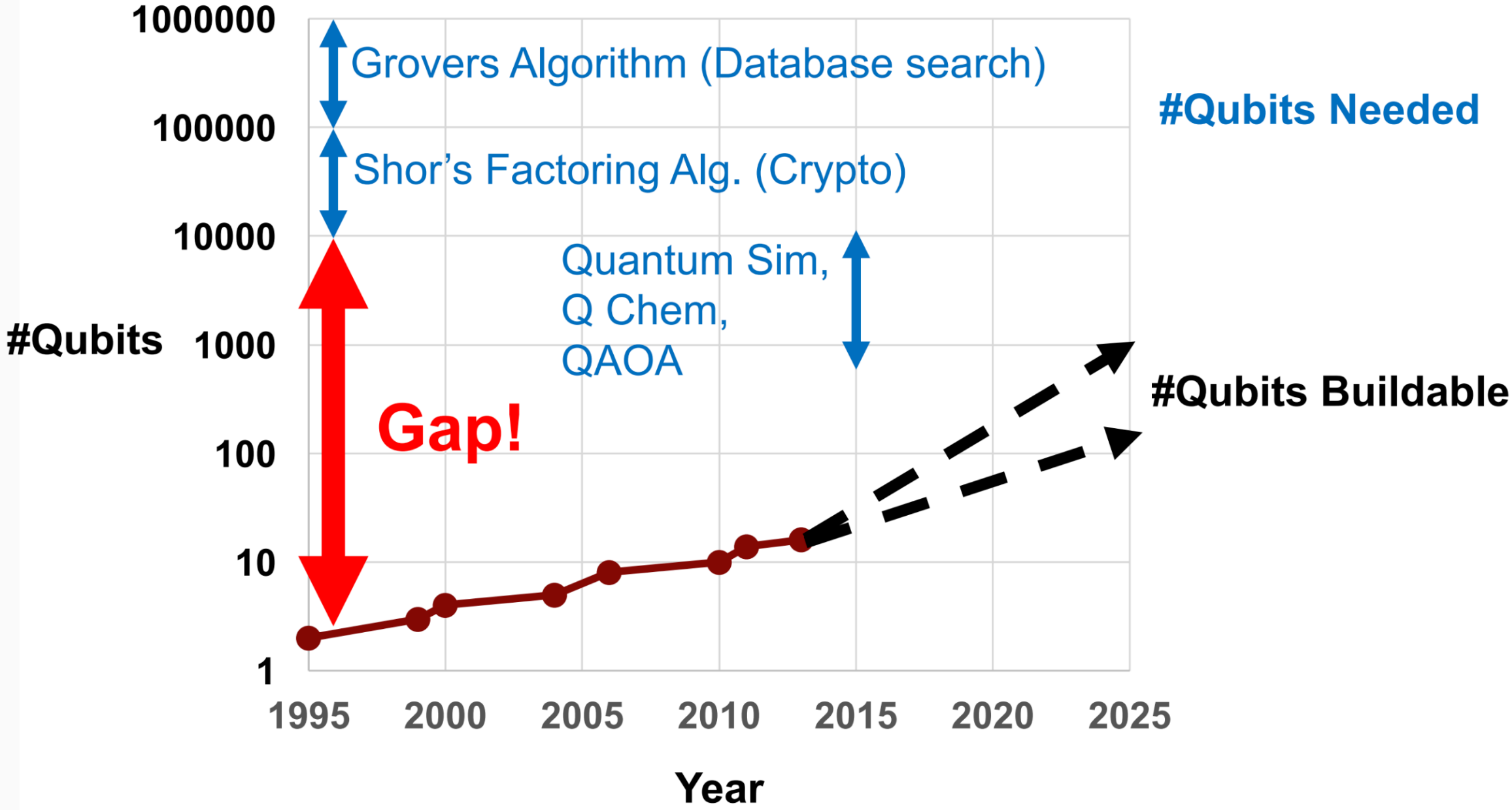
量子電腦的挑戰

演算法上，量子電腦只對特定某些問題，有相較古典演法上有優勢

- 例如：模擬量子系統、質因數分解 (Shor algorithm)、search problem (Grover algorithm)

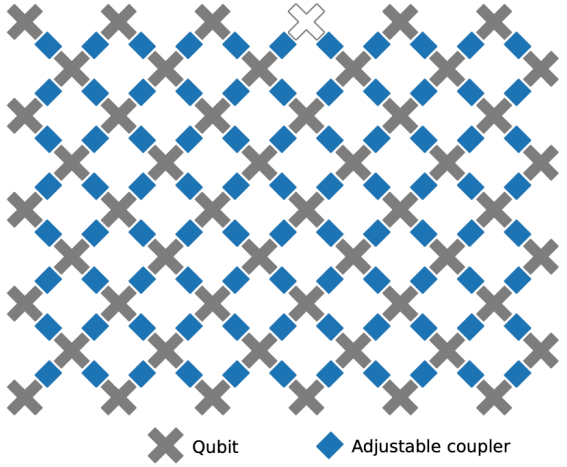
實作上，量子位元的數量及穩定度不夠

- 數量而言，要能建構出數量龐大，又可以讓任意兩個位元糾纏，工程難度高
- 穩定度而言，量子位元容易被環境雜訊干擾。因此，需要容錯計算
- 若使用容錯計算，需要以數百或數千個實體位元才能實作一個邏輯位元

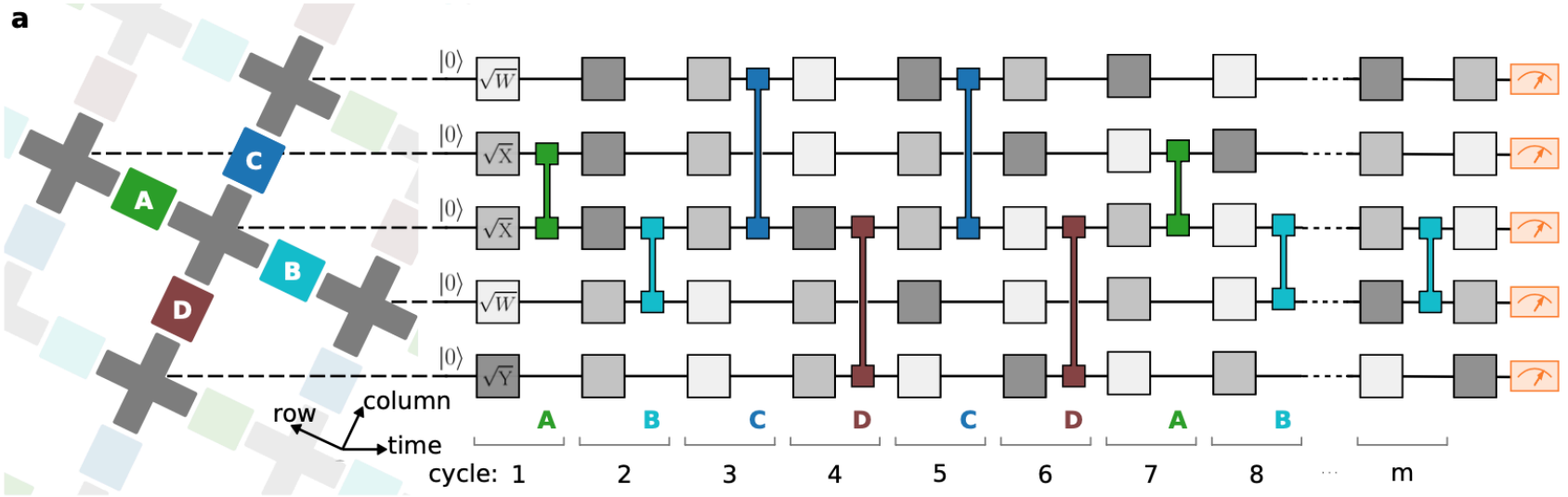


copy from: "Quantum Computing is Getting Real", by prof. Fred Chong at University of Chicago

Google 做了什麼？



- Google 使用 53 qubits 的量子電腦
- 隨機指定約20層的量子閘 (quantum gate)，並測量其運算結果
- 該計算可視為「從特定分布當中抽樣」(即特定分布的亂數產生器)
- 實驗重複一百萬次



量子電腦的迷思

Q: 量子電腦會不會取代傳統電腦、打敗超級電腦？

- A: 不會，量子電腦僅在特定問題上有優勢

Q: 網際網路還安全嗎？

- A: 安全，就算不安全也不是量子電腦害的 XD
- 量子電腦要破解現今使用的密碼系統，需要數十萬左右的實體量子位元
- 目前 NIST 已經在徵選「可以抵擋量子演算法的密碼系統」