꿈을 꾸는 양자 컴퓨팅

김명식

Imperial College London

Korea Institute for Advanced Study

SPRI, 26 April, Seoul

양자 테크놀로지 투자

- 미국, 중국, 유럽 정부: 각 연간 10억 달라 (1.37조) 투자

양자 테크놀로지

양자이론 (量子 理論, Quantum Theory) 을 바탕으로 새로운 정보통신 기술 개발

- 양자 컴퓨터
- 양자 센서 / 양자 navigator
- 양자 비밀 통신

양자 테크놀로지

양자이론 (**量子 理論**, Quantum Theory) 을 바탕으로 새로운 기술을 개발

- 양자 컴퓨터
- 양자 센서 / 양자 navigator: 정밀(정확한 위치, 정확한 문제점 측정) 의료, 보안, 국방 센서
- 양자 비밀 통신 : 도청 불가능한 비밀 통신. Toshiba, IDQ (Swiss), KT, SK 등 시장 판매 중

양자 테크놀로지 투자 : 정말 많은 걸까?

- 미국, 중국, 유럽 정부: 각 연간 10억 달라 (1.37조) 투자
- 참조: 1960년대 소련/미국 우주 경쟁시, 미국 우주 프로그램은 연방 예산의 4% 현재 10억 달라는 연방 예산의 0.01%.

양자 테크놀로지

양자이론 (**量子 理論,** Quantum Theory) 을 바탕으로 새로운 기술을 개발

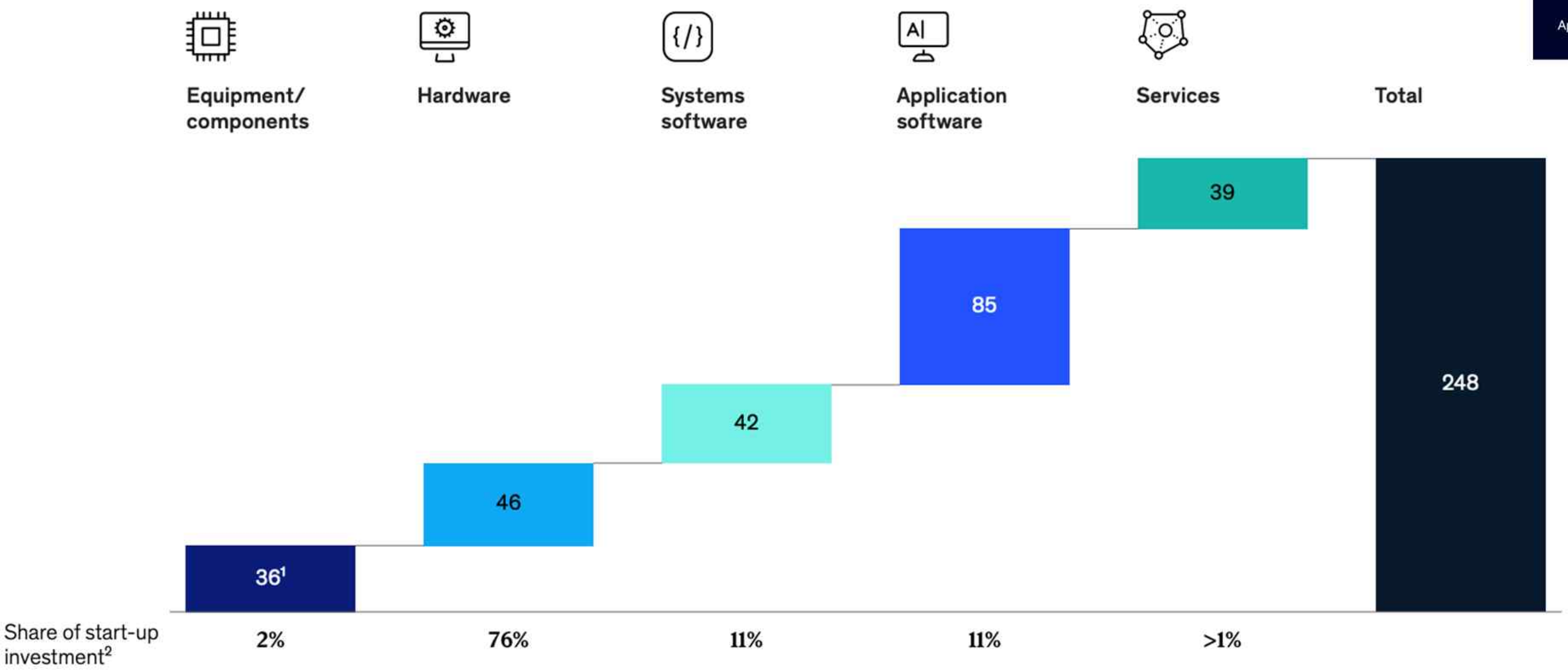
- **양자 컴퓨터**
- 양자 센서 / 양자 navigator: 정밀(정확한 위치, 정확한 문제점 측정) 의료, 보안, 국방 센서
- 양자 비밀 통신 : 도청 불가능한 비밀 통신. Toshiba, IDQ (Swiss), KT, SK 등 시장 판매 중

양자 컴퓨터 투자

- 미국, 중국, 유럽 정부: 각 연간 10억 달라 (1.37조) 투자
- **참조: 1960년대 소련/미국 우주 경쟁시, 미국 우주 프로그램은 연방 예산의 4% 현재 10억 달라는 연방 예산의 0.01%.**
- IBM, Google, Microsoft, Intel, NVIDIA 등 대기업,
- Photons: PsiQuantum ($600M), Xanadu ($200M), Quandela ($71M)
- Atoms: QuantEra ($20M), PasQal ($150M)
- Ions: IonQ, Universal Quantum, Oxford IoniQ

2022년 현재 북미+유럽에 200개의 quantum computing 스타트업

Number of QC start-ups, by value-chain segment

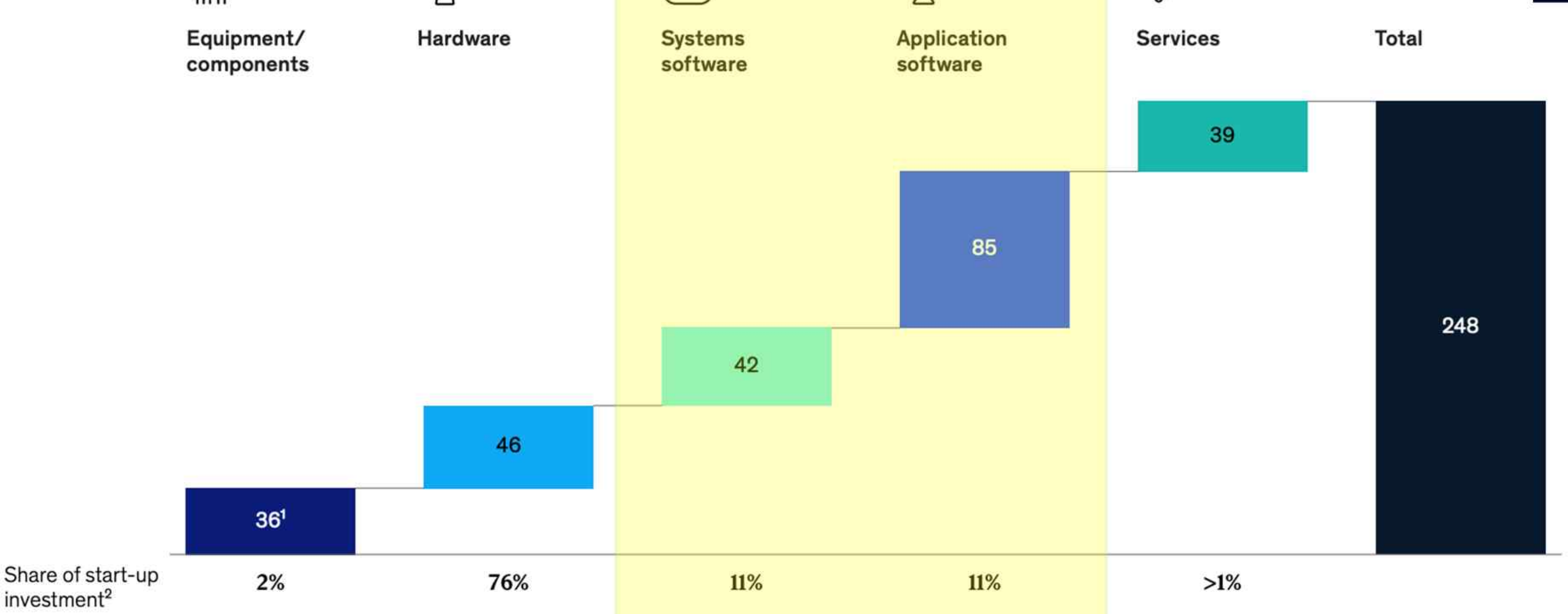


McKinsey & Company

Quantum Technology Monitor

April 2023

Number of QC start-ups, by value-chain segment

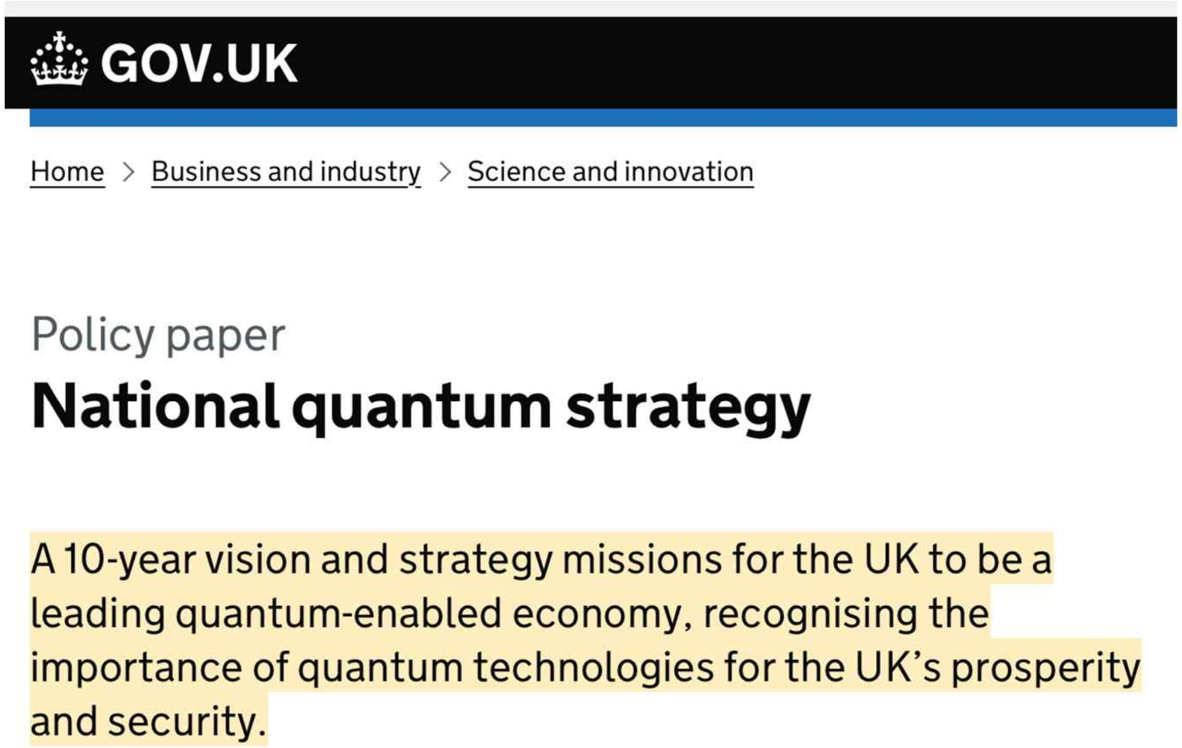


McKinsey & Company

Quantum Technology Monitor

April 2023

양자, 왜?



GOV.UK

Home > Business and industry > Science and innovation

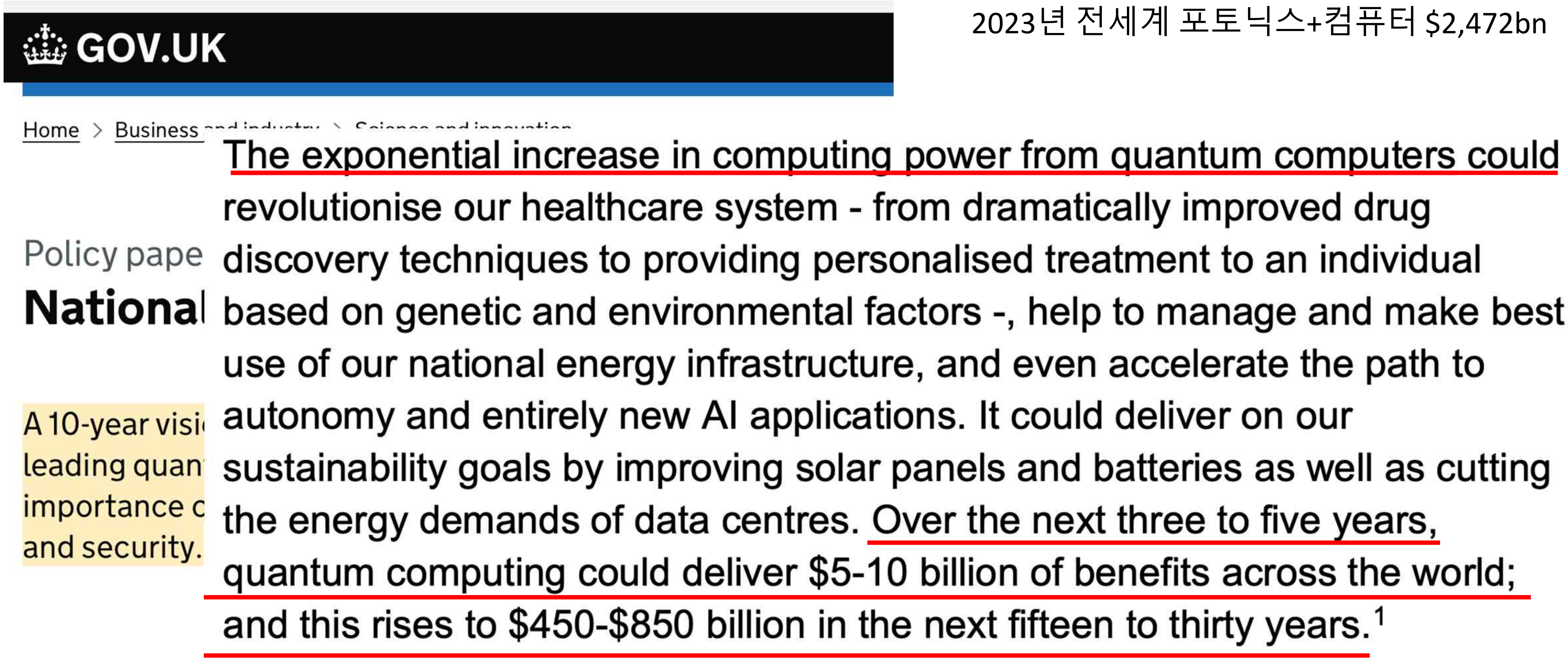
Policy paper

National quantum strategy

A 10-year vision and strategy missions for the UK to be a leading quantum-enabled economy, recognising the importance of quantum technologies for the UK's prosperity and security.

양자, 왜?

양자컴: 2차 양자 혁명
레이저, 트랜지스터: 1차양자혁명
2023년 전세계 포토닉스+컴퓨터 $2,472bn



GOV.UK

Home > Business and industry > Science and innovation

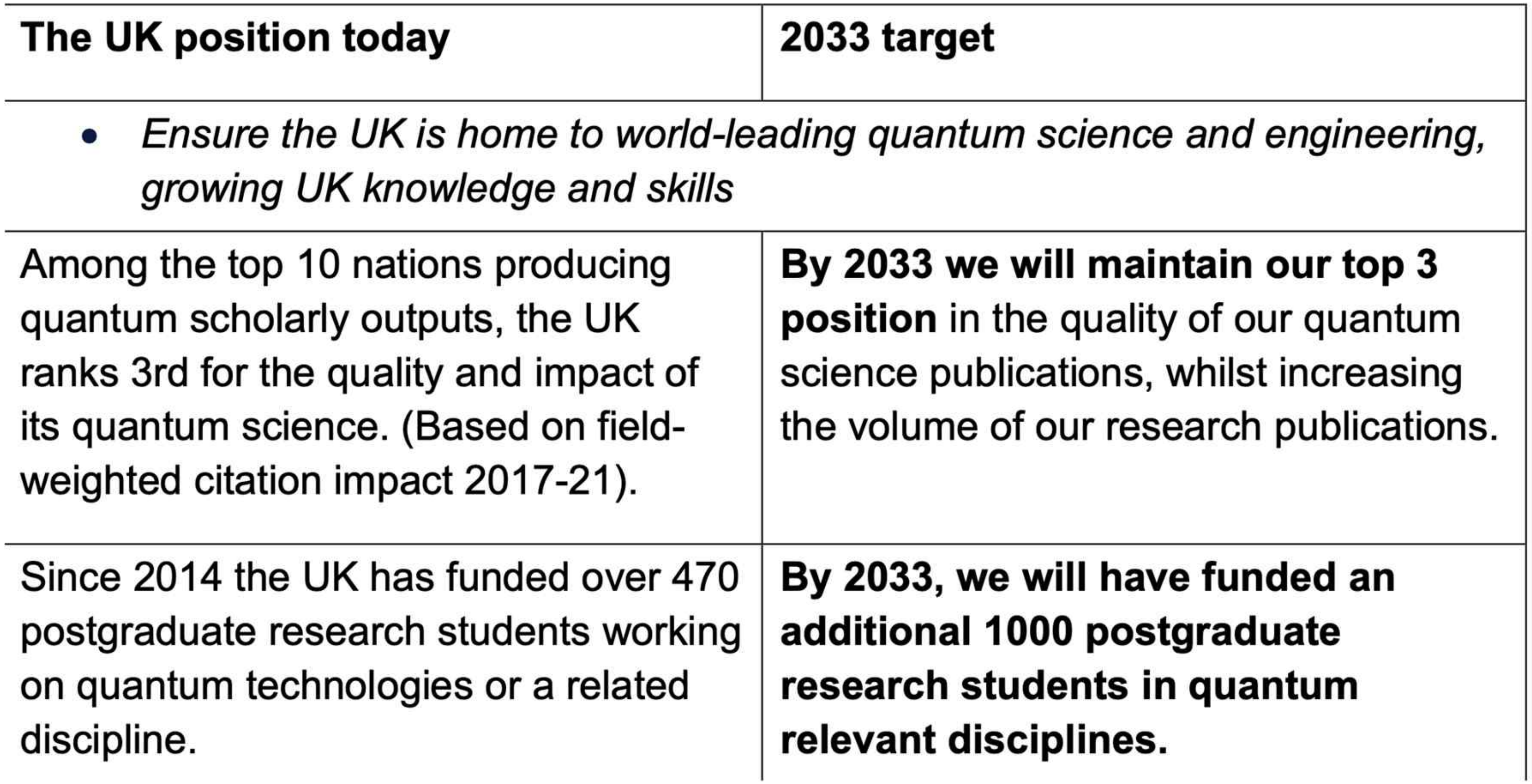
Policy pape

National

A 10-year visi
leading quan
importance c
and security.

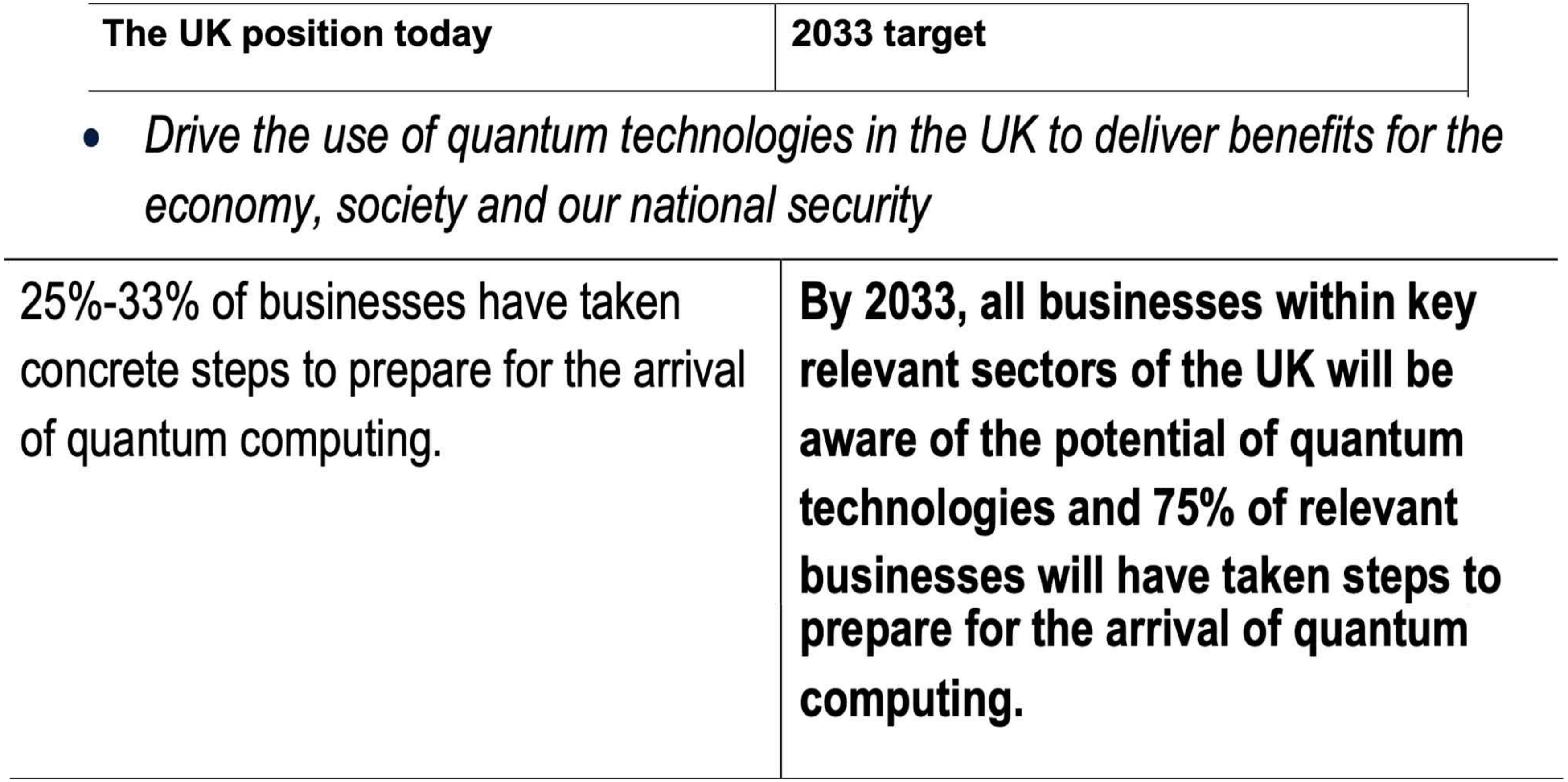
The exponential increase in computing power from quantum computers could revolutionise our healthcare system - from dramatically improved drug discovery techniques to providing personalised treatment to an individual based on genetic and environmental factors -, help to manage and make best use of our national energy infrastructure, and even accelerate the path to autonomy and entirely new AI applications. It could deliver on our sustainability goals by improving solar panels and batteries as well as cutting the energy demands of data centres. Over the next three to five years, quantum computing could deliver $5-10 billion of benefits across the world; and this rises to $450-$850 billion in the next fifteen to thirty years.[1]

영국 양자전략의 목적



The UK position today	2033 target
- *Ensure the UK is home to world-leading quantum science and engineering, growing UK knowledge and skills*	
Among the top 10 nations producing quantum scholarly outputs, the UK ranks 3rd for the quality and impact of its quantum science. (Based on field-weighted citation impact 2017-21).	**By 2033 we will maintain our top 3 position** in the quality of our quantum science publications, whilst increasing the volume of our research publications.
Since 2014 the UK has funded over 470 postgraduate research students working on quantum technologies or a related discipline.	**By 2033, we will have funded an additional 1000 postgraduate research students in quantum relevant disciplines.**

영국 양자전략의 목적



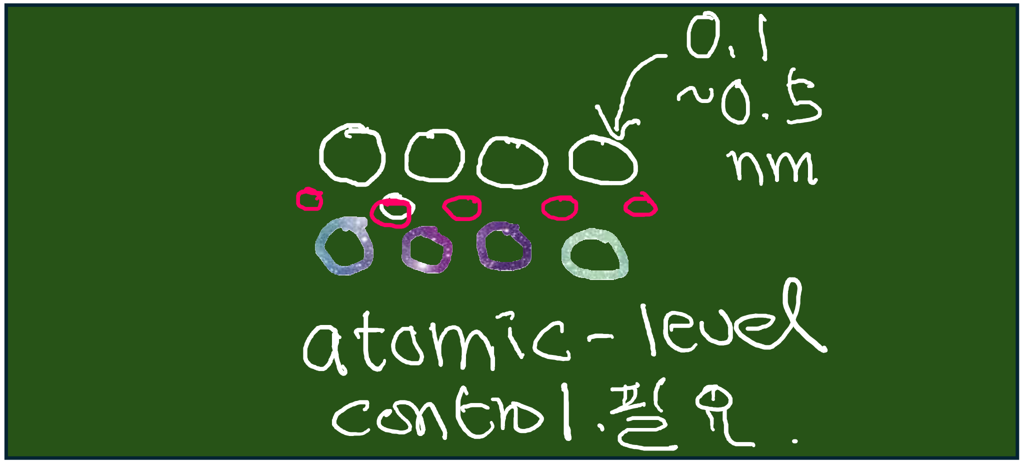
The UK position today	2033 target

- *Drive the use of quantum technologies in the UK to deliver benefits for the economy, society and our national security*

25%-33% of businesses have taken concrete steps to prepare for the arrival of quantum computing.	**By 2033, all businesses within key relevant sectors of the UK will be aware of the potential of quantum technologies and 75% of relevant businesses will have taken steps to prepare for the arrival of quantum computing.**

양자 컴퓨터: 왜?

- Shor’s algorithm (factoring a large number)
- 지속성 있는 발전을 위한 획기적인 테크놀로지의 필요성 : 에너지, 기후변화 등에 대한 과학적인 breakthrough 필요
- 국제적인 과학 경쟁 (예, 미국 대 중국)



양자 컴퓨터

- 양자 이론을 바탕으로 계산을 하는 컴퓨터
- 장점: 병렬 연산 가능 (예, 입력 0,1,2,3…에 대해 동시에 함수값 f(0), f(1), f(2)… 등 계산하고 이들의 함수 g(f(0), f(1),…) 등도 계산 할 수 있다.) 진정한 병렬 연산
- 단점: 계산한 값을 다 출력하지 않는다.

병렬 연산

Serial processing

병렬 연산

양자병렬 연산이 무슨 일을 더 잘 할 수 있을까?

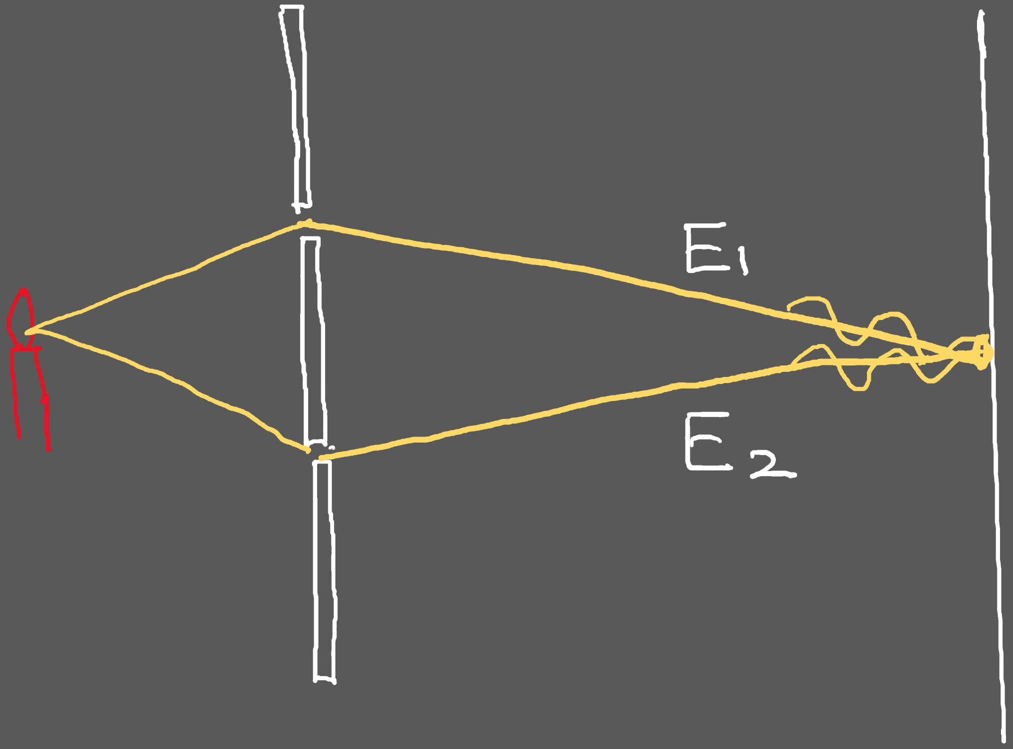
Serial processing

간단한 양자 이론

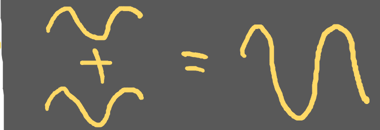
- 어떠한 시스템이 양자 이론에 따른다면 그 시스템은 파동성과 입자성을 동시에 가진다.
- 파동성: 간섭을 한다.
- 입자성: 덩어리로 되어 있고 셀 수 있다.
- 양자 컴퓨터는 파동성으로 계산을 하고, 입자성으로 출력을 낸다.

St George's hospital, London

Thomas Young의 이중 슬릿 간섭



$$|E_1 + E_2|^2 = 4E_1^2$$
$$(\text{if } E_1 = E_2)$$

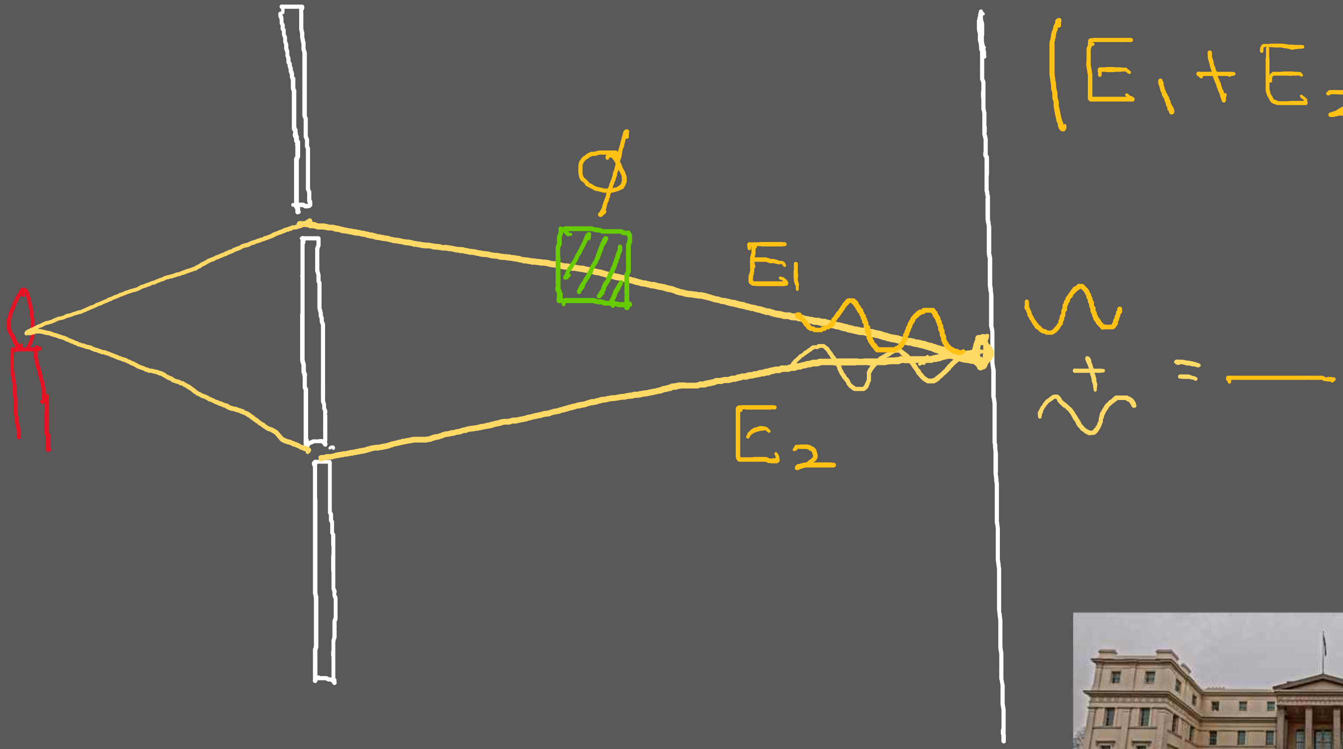


bright

St George's hospital, London

Thomas Young, a great polymath.

Thomas Young의 이중 슬릿 간섭



$$|E_1+E_2|^2 = |E_1 e^{i\phi}+E_1|^2$$

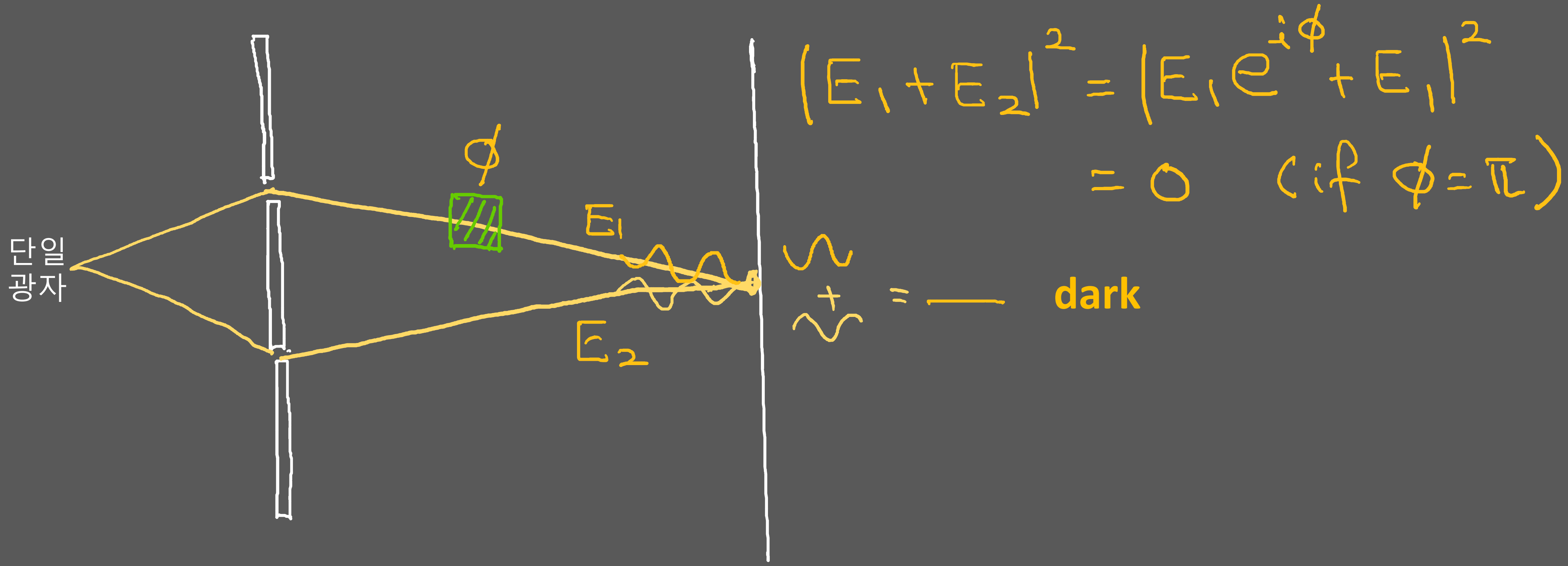
$$= 0 \quad (\text{if } \phi = \pi)$$

dark

St George's hospital, London

Thomas Young, a great polymath.

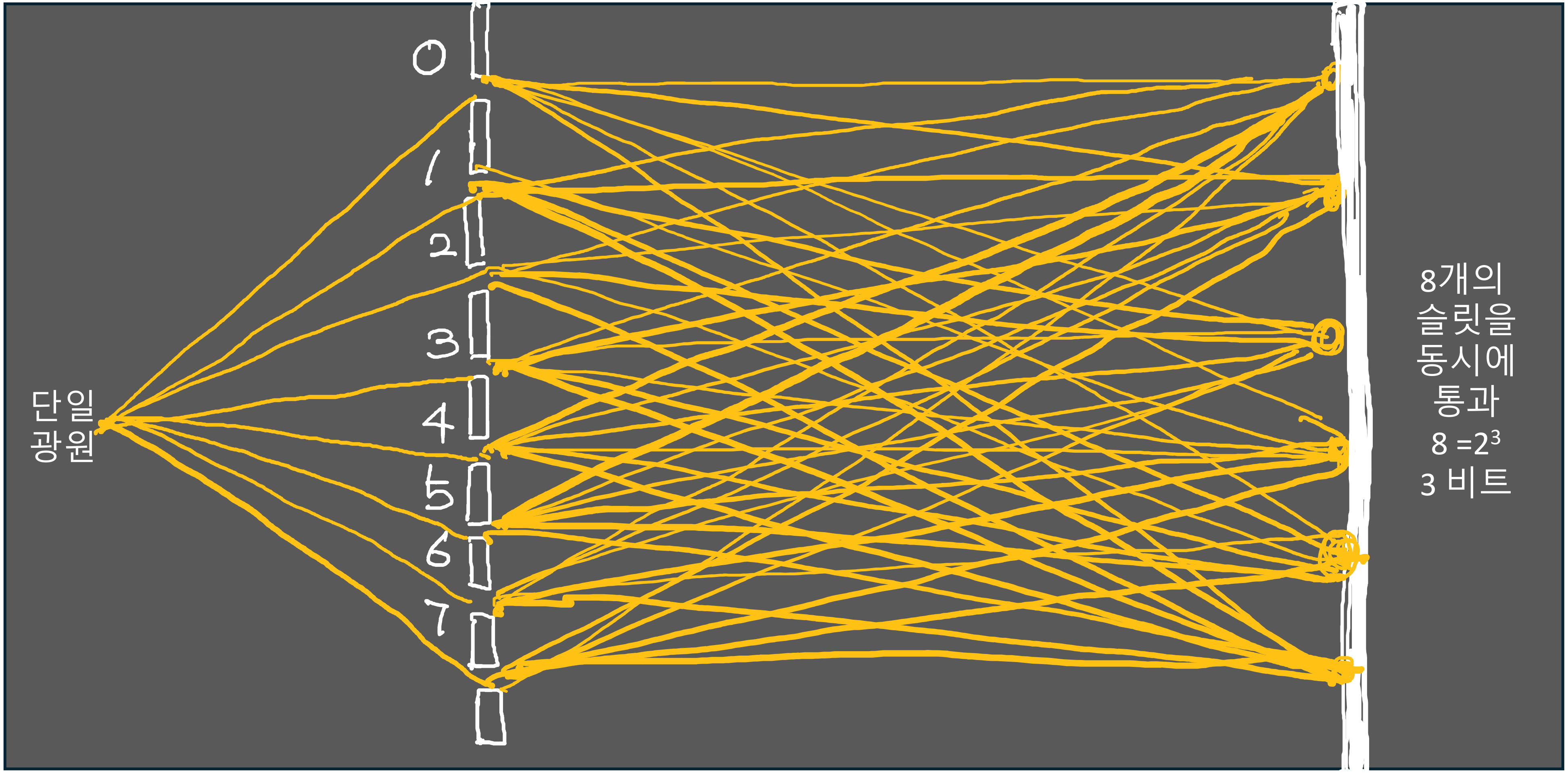
양자 이중 슬릿 간섭



$$|E_1+E_2|^2 = |E_1 e^{i\phi} + E_1|^2$$
$$= 0 \quad (\text{if } \phi = \pi)$$

한개의 입자(단일광자)가 두개의 슬릿을 동시에 지나 간섭을 일으킨다.
한개의 비트가 0과 1을 동시에 가지고, ϕ가 있는지 알아낸다.

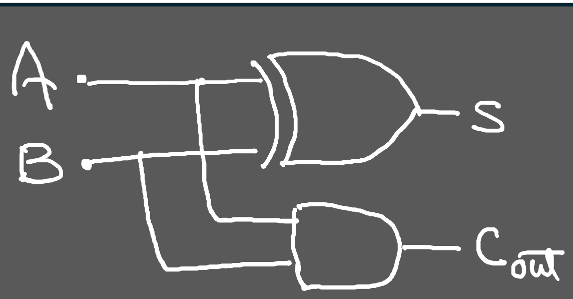
양자 간섭 일반화 (양자 병렬연산)



8개의
슬릿을
동시에
통과
$8 = 2^3$
3 비트

간단한 예: 덧셈

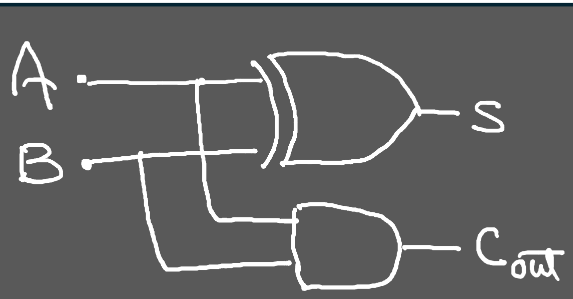
기존 컴퓨터



Inputs		Outputs	
A	B	S	C_{out}
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

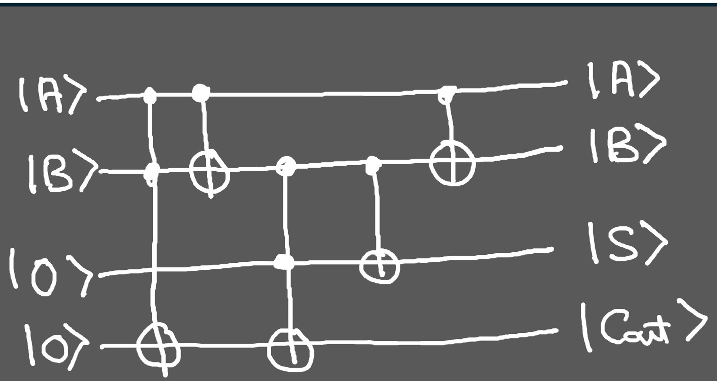
간단한 예: 덧셈

기존 컴퓨터



Inputs		Outputs	
A	B	S	C_{out}
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

양자컴퓨터

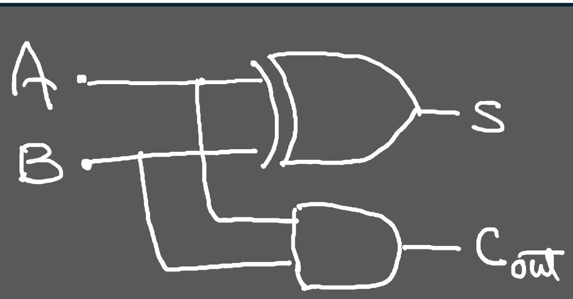


Input |AB> ; Output |S C_{out}>

|AB>|00> → |AB>|S C_{out}>

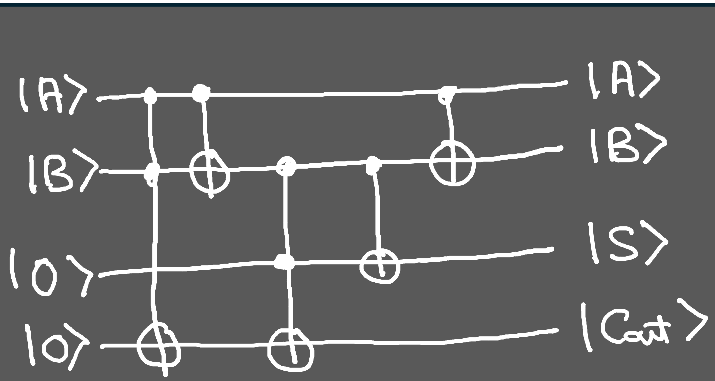
간단한 예: 덧셈

기존 컴퓨터



Inputs		Outputs	
A	B	S	C_{out}
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

양자컴퓨터



|AB>|00> → |AB>|S C_{out}>

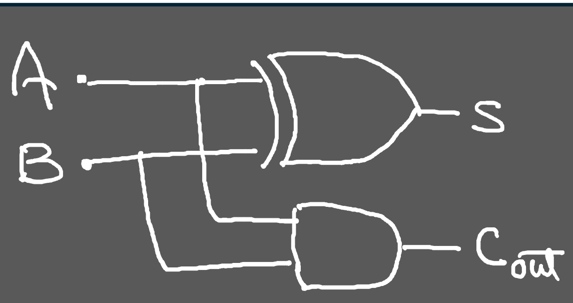
$(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|0\rangle|0\rangle$

→

$|0\rangle|0\rangle\ |0\rangle|0\rangle + |0\rangle|1\rangle\ |1\rangle|0\rangle$
$+ |1\rangle|0\rangle\ |1\rangle|0\rangle + |1\rangle|1\rangle\ |0\rangle|1\rangle$

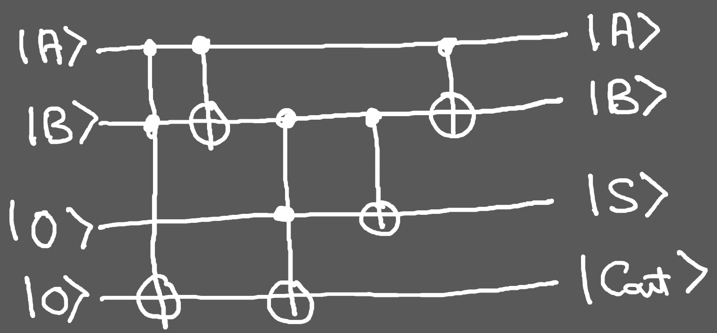
간단한 예: 덧셈

기존 컴퓨터



Inputs		Outputs	
A	B	S	C_{out}
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

양자컴퓨터



$(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|0\rangle|0\rangle$

→

$|0\rangle|0\rangle\ |0\rangle|0\rangle + |0\rangle|1\rangle\ |1\rangle|0\rangle$

$+ |1\rangle|0\rangle\ |1\rangle|0\rangle + |1\rangle|1\rangle\ |0\rangle|1\rangle$

병렬 연산 가역 연산

전혀 다른 로직 게이트

양자로직 게이트

- 양자 상태: 벡터 $\begin{pmatrix}1\\0\end{pmatrix}$ $\begin{pmatrix}0\\1\end{pmatrix}$ $\begin{pmatrix}1\\1\end{pmatrix}$
- 양자 로직게이트: 행렬 $\begin{pmatrix}1 & 0\\0 & e^{i\phi}\end{pmatrix}$, $\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$
- 연산

$$\begin{pmatrix}1\\e^{i\phi}\end{pmatrix}=\begin{pmatrix}1 & 0\\0 & e^{i\phi}\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}$$

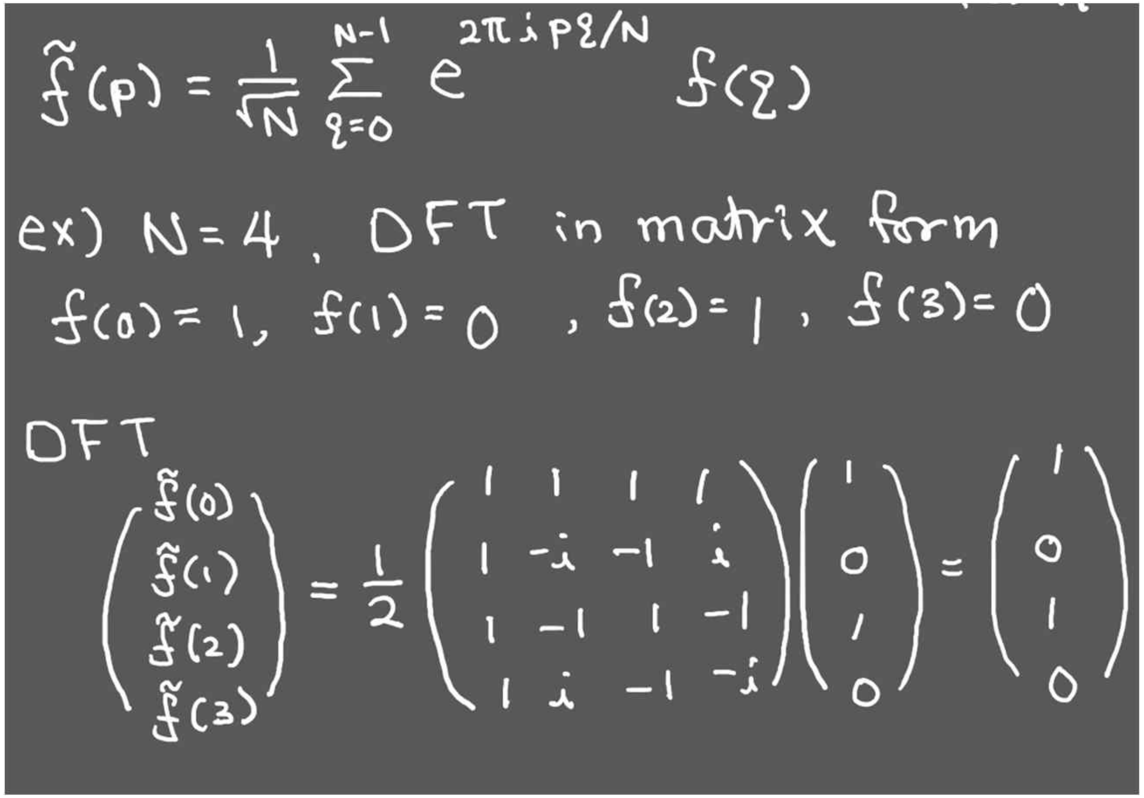
양자로직 게이트

- 양자 상태: 벡터 $\begin{pmatrix}1\\0\end{pmatrix}$ $\begin{pmatrix}0\\1\end{pmatrix}$ $\begin{pmatrix}1\\1\end{pmatrix}$
- 양자 로직게이트: 행렬 $\begin{pmatrix}1 & 0\\0 & e^{i\phi}\end{pmatrix}$, $\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$
- 연산

$$\begin{pmatrix}1\\e^{i\phi}\end{pmatrix}=\begin{pmatrix}1 & 0\\0 & e^{i\phi}\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}$$

행렬, 벡터 계산을 한번에 ---Machine learning, AI 와 연관성?

Discrete Fourier Transform



$$\tilde{f}(p) = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{2\pi i p q / N} f(q)$$

ex) $N=4$, DFT in matrix form

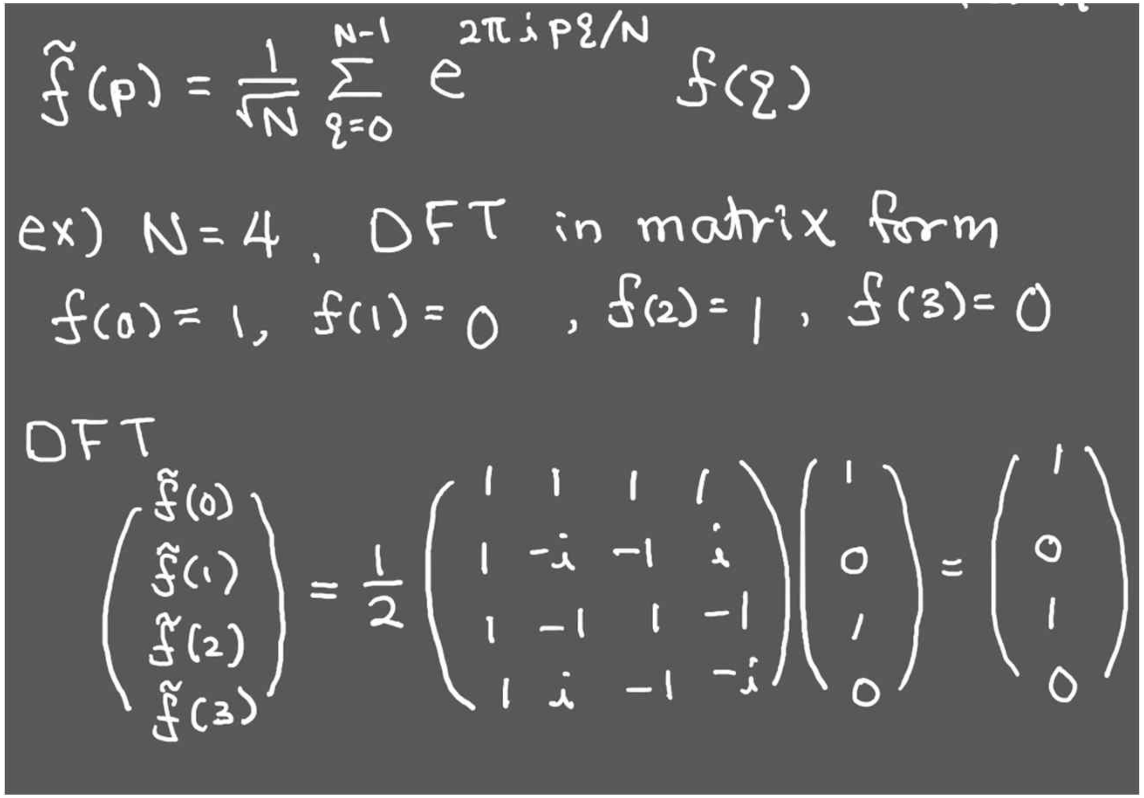
$f(0)=1$, $f(1)=0$, $f(2)=1$, $f(3)=0$

DFT

$$\begin{pmatrix} \tilde{f}(0) \\ \tilde{f}(1) \\ \tilde{f}(2) \\ \tilde{f}(3) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Computational complexity $\mathcal{O}(n)$

Discrete Fourier Transform



$$\tilde{f}(p) = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{2\pi i p q/N} f(q)$$

ex) $N=4$, DFT in matrix form

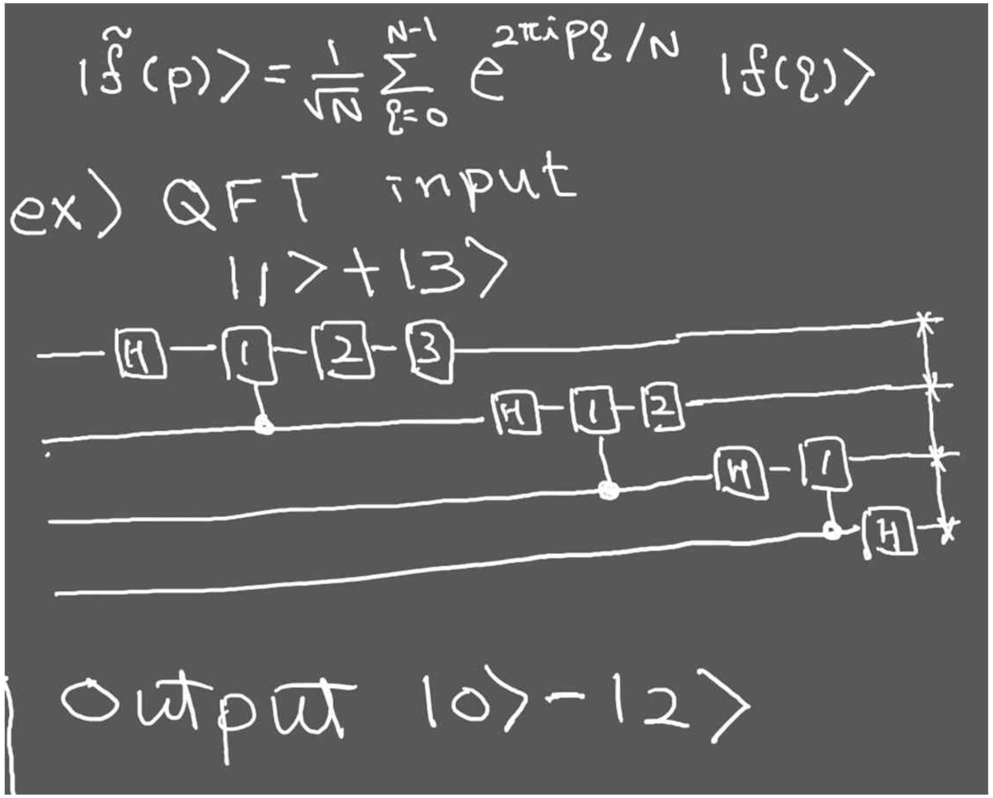
$f(0)=1$, $f(1)=0$, $f(2)=1$, $f(3)=0$

DFT

$$\begin{pmatrix} \tilde{f}(0) \\ \tilde{f}(1) \\ \tilde{f}(2) \\ \tilde{f}(3) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Computational complexity $\mathcal{O}(n)$

Quantum Fourier Transform



$$|\tilde{f}(p)\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{2\pi i p q/N} |f(q)\rangle$$

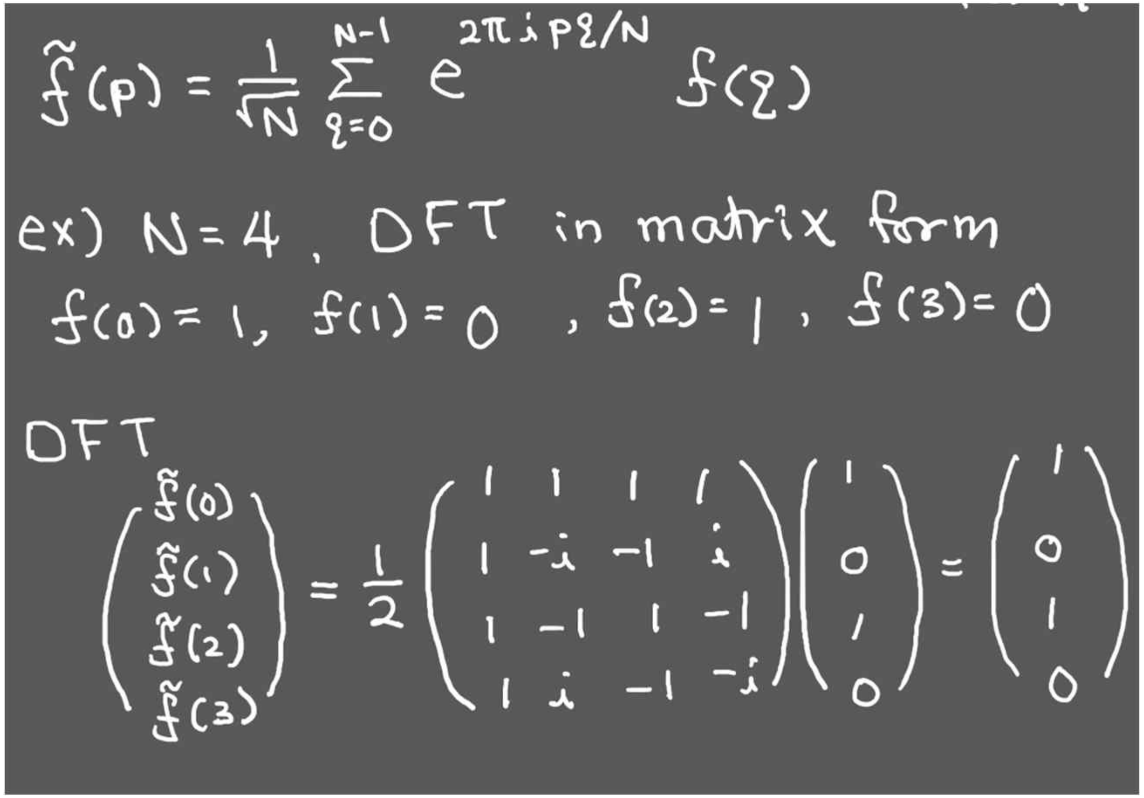
ex) QFT input

$|1\rangle + |3\rangle$

output $|0\rangle - |2\rangle$

Computational complexity $\mathcal{O}(\log n)^2$

Discrete Fourier Transform



$$\tilde{f}(p) = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{2\pi i pq/N} f(q)$$

ex) $N=4$, DFT in matrix form

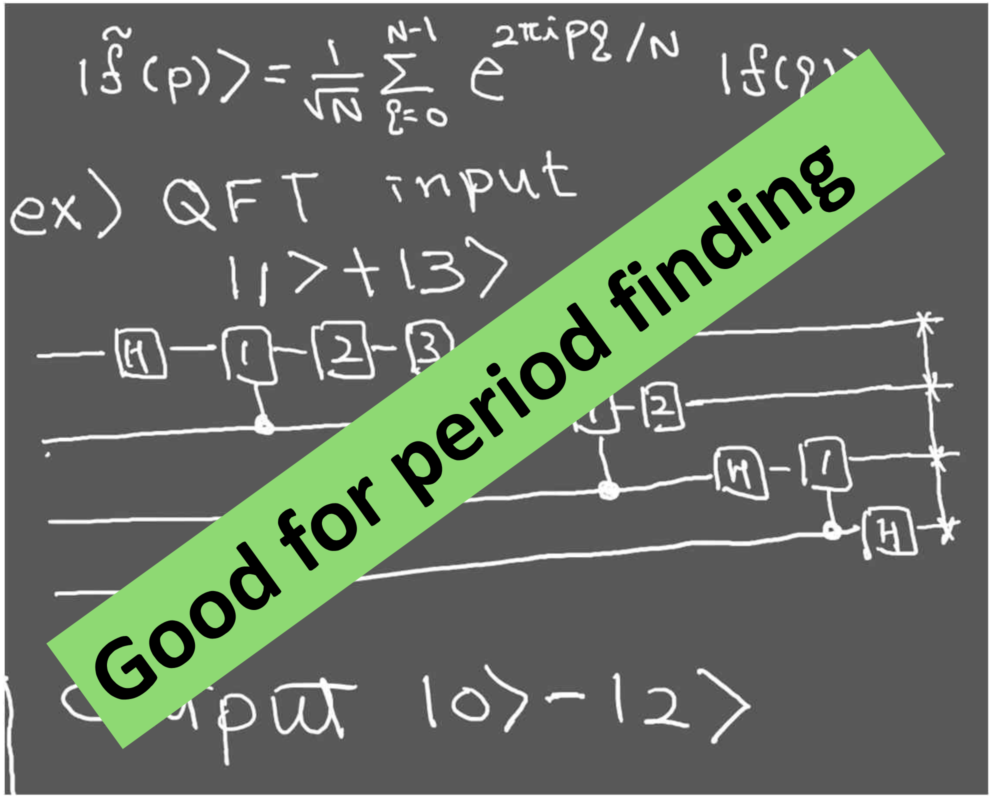
$f(0)=1$, $f(1)=0$, $f(2)=1$, $f(3)=0$

DFT

$$\begin{pmatrix} \tilde{f}(0) \\ \tilde{f}(1) \\ \tilde{f}(2) \\ \tilde{f}(3) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Computational complexity $\mathcal{O}(n)$

Quantum Fourier Transform



$$|\tilde{f}(p)\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} e^{2\pi i pq/N} |f(q)\rangle$$

ex) QFT input

$|1\rangle + |3\rangle$

output $|0\rangle - |2\rangle$

Good for period finding

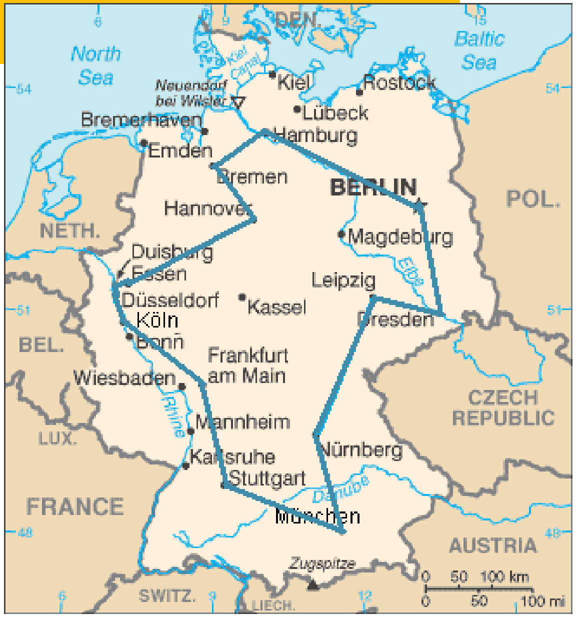
Computational complexity $\mathcal{O}(\log n)^2$

Quantum 알고리즘

- Shor's factoring algorithm
- Quantum period finding
- Quantum simulations
- Quantum random walks
- HHL to solve $A\vec{x}$ =$\vec{b} \rightarrow \vec{x} = A^{-1}\vec{b}$

15개의 독일 대도시를 다녀오는 최단거리?

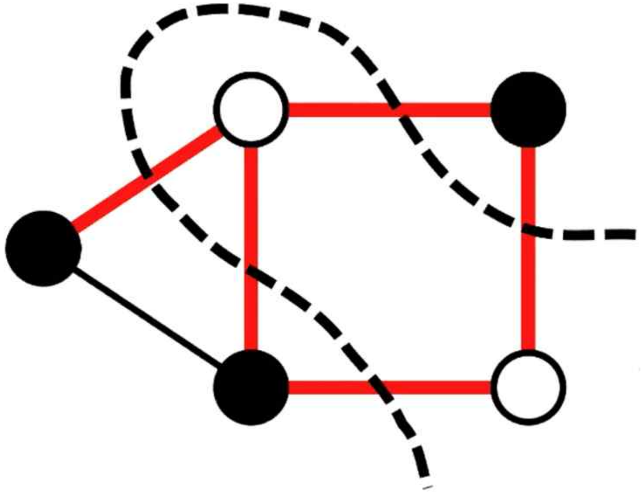
$$H(\vec{x}) = \sum_{\alpha,\beta\in\mathcal{S}} \sum_{i=1}^{N} w_{\alpha\beta} x_{\alpha,i} x_{\beta,i+1}$$



- Binary optimization $\in$combinatorial optimization
- Quadratic binary optimization
- Spin interaction model
- To optimize this is the same as to find the ground state

Qubo (Quantum unconstrained binary optimisation)

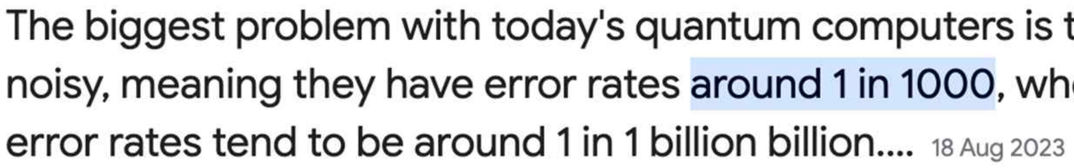
Max-cut problem



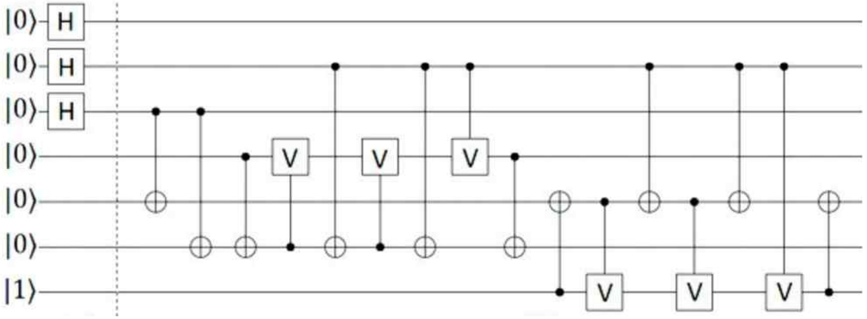
$$H_e = \frac{1}{2}(1 - \sigma_z^u \sigma_z^v)$$

QAOA: Quantum approximate optimization algorithm

양자컴퓨터를 만드는데 난점은?



The biggest problem with today's quantum computers is that they are noisy, meaning they have error rates around 1 in 1000, whereas classical error rates tend to be around 1 in 1 billion billion.... 18 Aug 2023



- Errors
- 1% error → after 100 gate operations 63.3% error
- 0.1% error → after 100 gate operations 10% error
- 0.01% error → after 100 gate operations 1% error, 1000 gate 10%

오류보정

- Correcting errors by measurements and feedback

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

- If there is a bit flip error in the qubmit one: $\alpha|1\rangle|0\rangle|0\rangle + \beta|0\rangle|1\rangle|1\rangle$

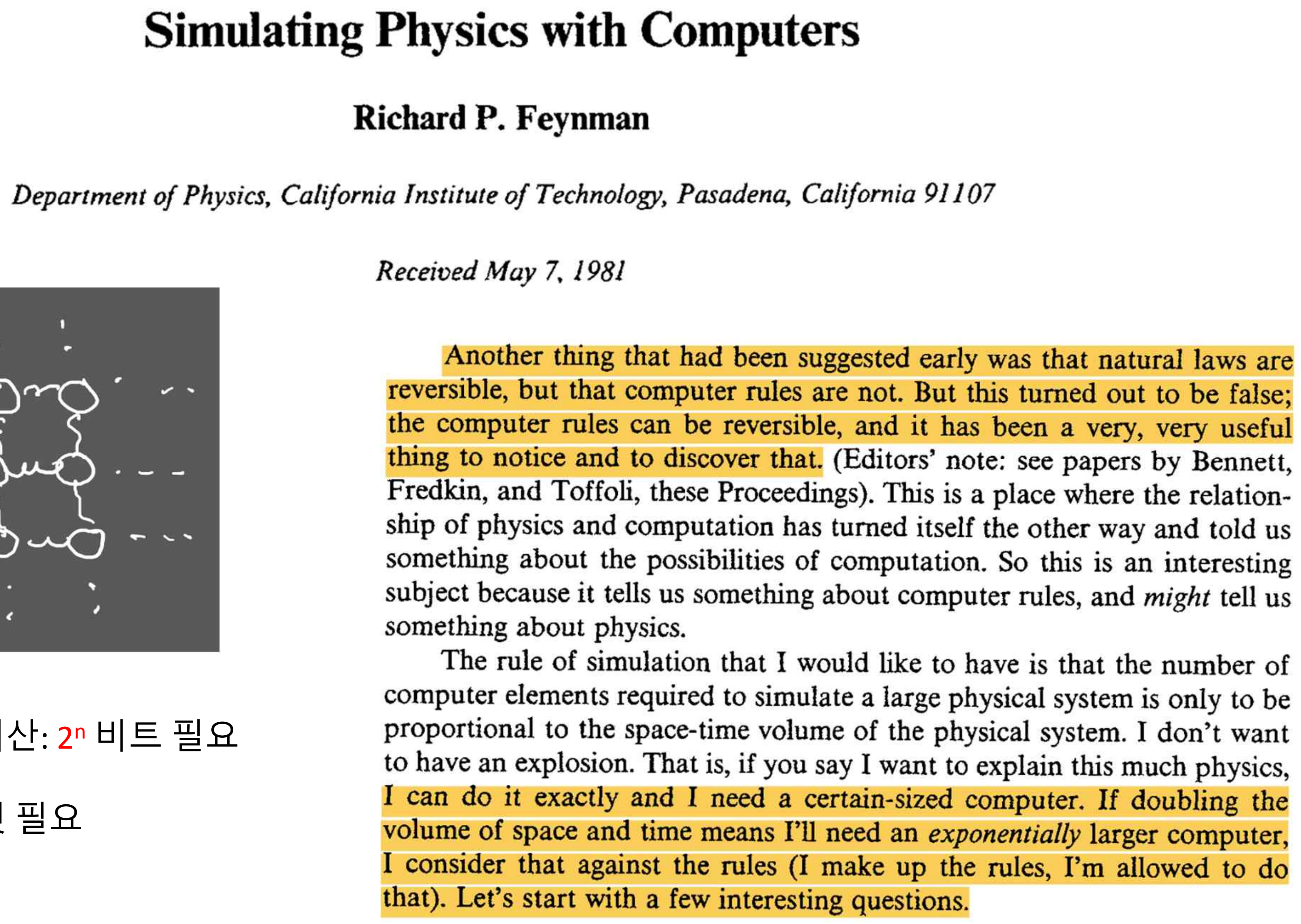
- By the Z_1 Z_2 measurement, we get -1 rather than 1 so we know that either qubit 1 or qubit 2 flipped. By the Z_2 Z_3 measurement, we get +1 value, so we know that qubit 1 flipped. So we can correct it by applying X_1 operation.

오류보정

- a|0>+b|1>: Once we measure in {0,1} basis, the superposition is lost. No way to correct the error
- a|00>+b|11>: We measure {{00,11}, {01, 10}} basis, {01,10} measurement outcomes indicate that an error took place but we do not know where.
- a|000>+b|111>: We measure {{00,11}, {01,10}} basis for 1st and 2nd qubits, then the same for 2nd and 3rd qubits. We will be able to identify where the error took place. Then we can correct it.

Quantum simulation

- Simulation of highly correlated systems
  - High T Superconductivity
- Simulation of quantum dynamics
  - Batteries
  - Solar cells



Simulating Physics with Computers

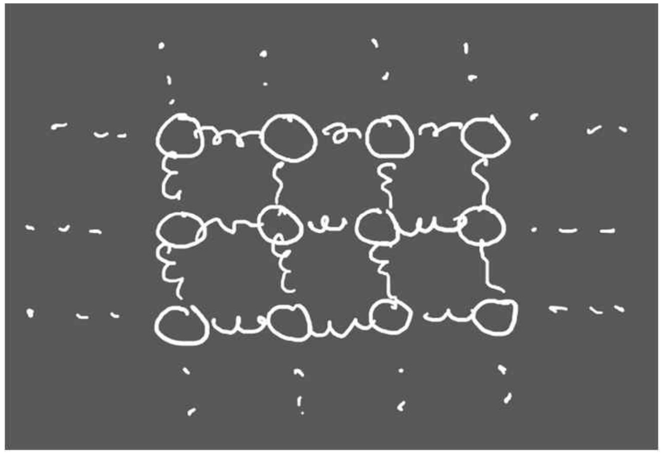
Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

Another thing that had been suggested early was that natural laws are reversible, but that computer rules are not. But this turned out to be false; the computer rules can be reversible, and it has been a very, very useful thing to notice and to discover that. (Editors' note: see papers by Bennett, Fredkin, and Toffoli, these Proceedings). This is a place where the relationship of physics and computation has turned itself the other way and told us something about the possibilities of computation. So this is an interesting subject because it tells us something about computer rules, and *might* tell us something about physics.

The rule of simulation that I would like to have is that the number of computer elements required to simulate a large physical system is only to be proportional to the space-time volume of the physical system. I don't want to have an explosion. That is, if you say I want to explain this much physics, I can do it exactly and I need a certain-sized computer. If doubling the volume of space and time means I'll need an *exponentially* larger computer, I consider that against the rules (I make up the rules, I'm allowed to do that). Let's start with a few interesting questions.



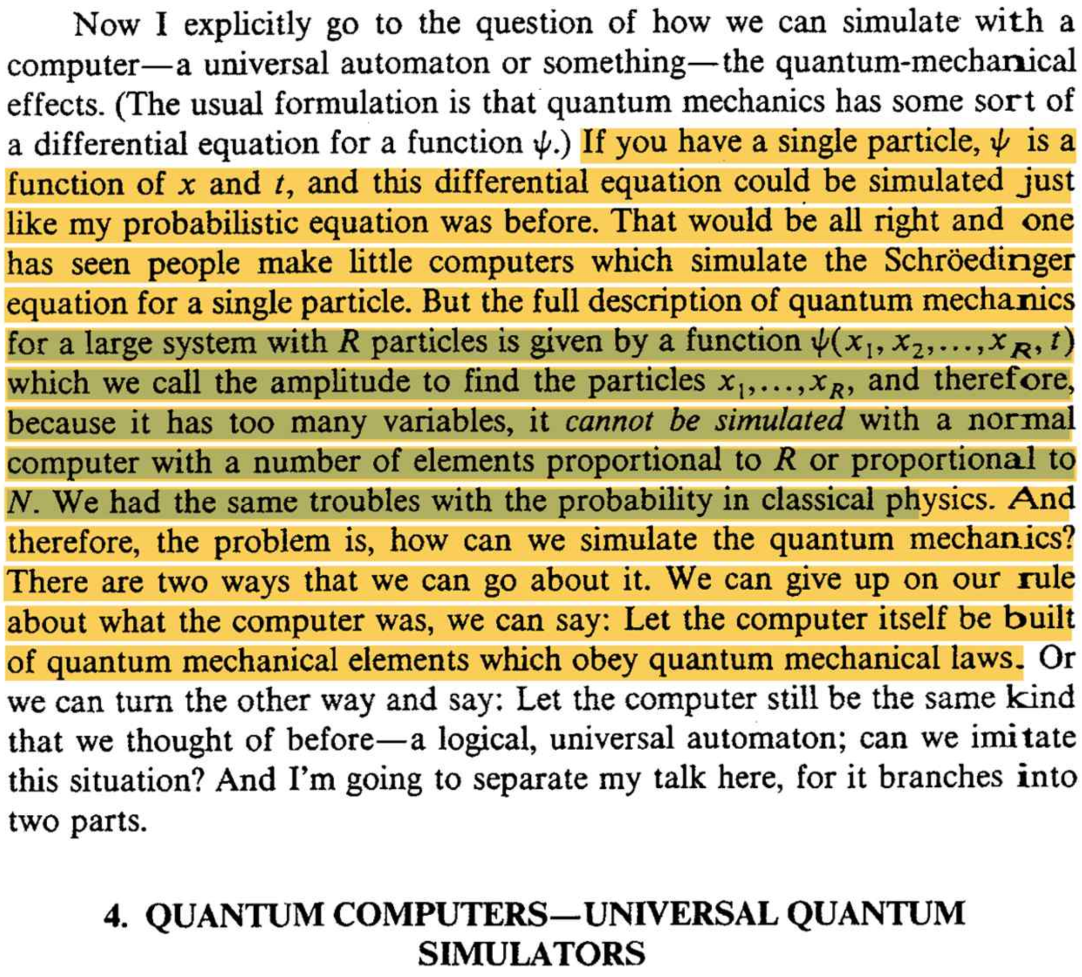
n 개의 2준위 원자 계산: 2^n 비트 필요

양자컴은 n개의 큐빗 필요

양자상태는 negative 확률을
가질 수도.

상용컴퓨터로 계산이 어려울 수
있다.

양자 계산이 필요할 때 상용컴퓨터는
한계가 있을 수 있다.

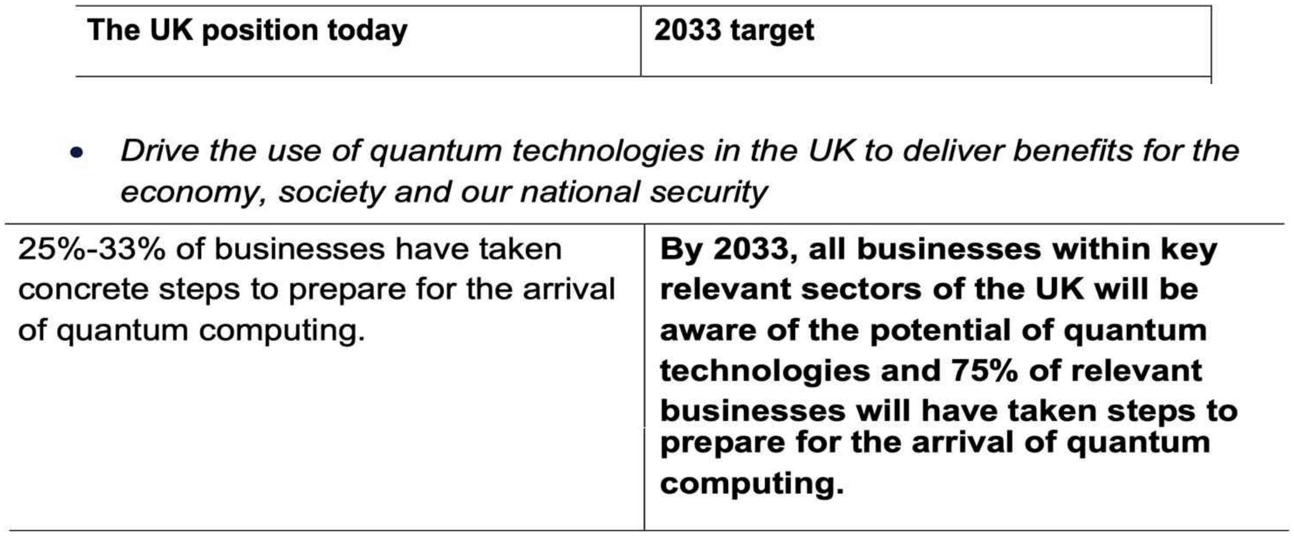


Now I explicitly go to the question of how we can simulate with a computer—a universal automaton or something—the quantum-mechanical effects. (The usual formulation is that quantum mechanics has some sort of a differential equation for a function ψ.) If you have a single particle, ψ is a function of x and t, and this differential equation could be simulated just like my probabilistic equation was before. That would be all right and one has seen people make little computers which simulate the Schröedinger equation for a single particle. But the full description of quantum mechanics for a large system with R particles is given by a function $\psi(x_1, x_2, \ldots, x_R, t)$ which we call the amplitude to find the particles $x_1, \ldots, x_R$, and therefore, because it has too many variables, it *cannot be simulated* with a normal computer with a number of elements proportional to R or proportional to N. We had the same troubles with the probability in classical physics. And 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 we can turn the other way and say: Let the computer still be the same kind that we thought of before—a logical, universal automaton; can we imitate this situation? And I'm going to separate my talk here, for it branches into two parts.

4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS

양자 컴퓨터 원리와 응용

- Optimisation
  - Finance
  - Logistics
- Simulations
  - New materials
  - Drug design
- Calculating dynamics
  - Solar cells



The UK position today	2033 target
• *Drive the use of quantum technologies in the UK to deliver benefits for the economy, society and our national security*	
25%-33% of businesses have taken concrete steps to prepare for the arrival of quantum computing.	**By 2033, all businesses within key relevant sectors of the UK will be aware of the potential of quantum technologies and 75% of relevant businesses will have taken steps to prepare for the arrival of quantum computing.**

Justified Scepticism