Second Quantum Revolution

Univ. Santiago de Compostela
november 2016

José I. Latorre
Univ. Barcelona / National Univ. Singapore

UNIVERSITAT DE BARCELONA

NUS National University of Singapore

CENTRO DE CIENCIAS DE BENASQUE PEDRO PASCUAL

| Entanglement Partners_ >

IN THE NEWS

Google's D-Wave 2X Quantum Computer 100 Million Times Faster Than Regular Computer Chip

9 December 2015, 9:40 am EST By Alyssa Navarro Tech Times

Google and NASA engineers announced Tuesday that the D-Wave 2X quantum computer in Silicon Valley solved an optimization problem within mere seconds. With that, researchers want to enhance the calculations on the D-Wave 2X so the input into the machine can be easier. (NASA/Quantum Artificial Intelligence Laboratory)

Tapping into the ostensibly "magical fount" of quantum mechanics could possibly result to an outpouring of new and ground-breaking advancements in material science.

A team of Google and NASA engineers is at the heart of an incredibly significant finding that may someday lead to precisely that.

Deep within the space agency's Advanced Supercomputing center in Silicon Valley is a huge black box called D-Wave 2X Quantum Computer. It is a machine acquired by Google and NASA in 2013 which can decipher complex problems that classical computers cannot handle.

"We have already encountered problems we would like to solve that are unfeasible with conventional computers," said Google Vice President for Engineering John Giannandrea. "We

Hillary Clinton wants “Manhattan-like project” to break encryption

US should be able to bypass encryption—but only for terrorists, candidate says.

by **Jon Brodkin** - Dec 21, 2015 5:15pm CET

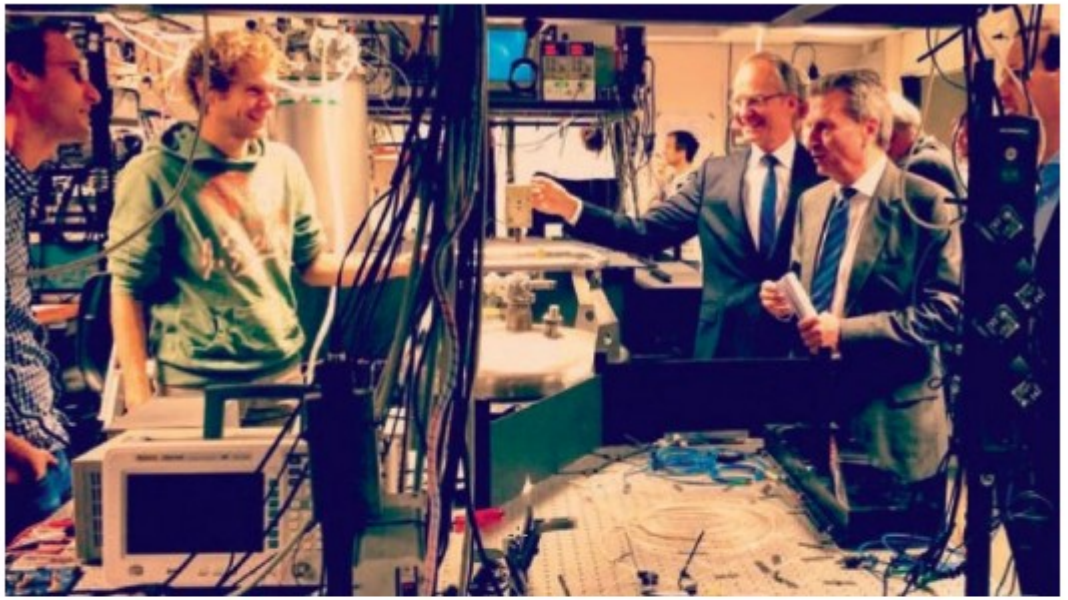
Enlarge / Hillary Clinton.

Clinton campaign.

Presidential candidate Hillary Clinton has called for a "Manhattan-like project" to help law enforcement break into encrypted communications. This is in reference to the Manhattan Project, the top-secret concentrated research effort which resulted in the US developing nuclear weapons during World War II.

At Saturday's Democratic debate (transcript here), moderator Martha Raddatz asked Clinton about Apple CEO Tim Cook's statements that any effort to break encryption would harm law-abiding citizens.

22/04/2016



Günther Oettinger, the European commissioner for digital economy, and Henk Kamp, the Dutch minister for economic affairs, visit the QuTech lab, a quantum technology laboratory in Delft, the Netherlands.

Quantum Manifesto

Europe to bet up to €1 billion on quantum technology

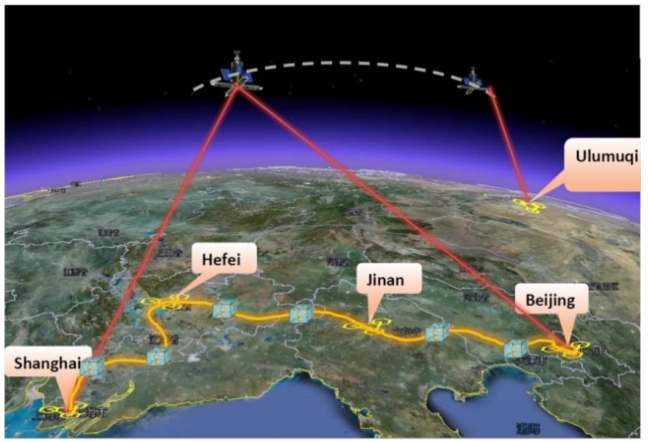
By **Kai Kupferschmidt** | Apr. 22, 2016 , 4:15 PM

Aproved on May 17

The European Commission has picked a third research area where it hopes to have a major impact by spending a massive amount of cash. Research groups across the continent will receive up to €1 billion over the

China

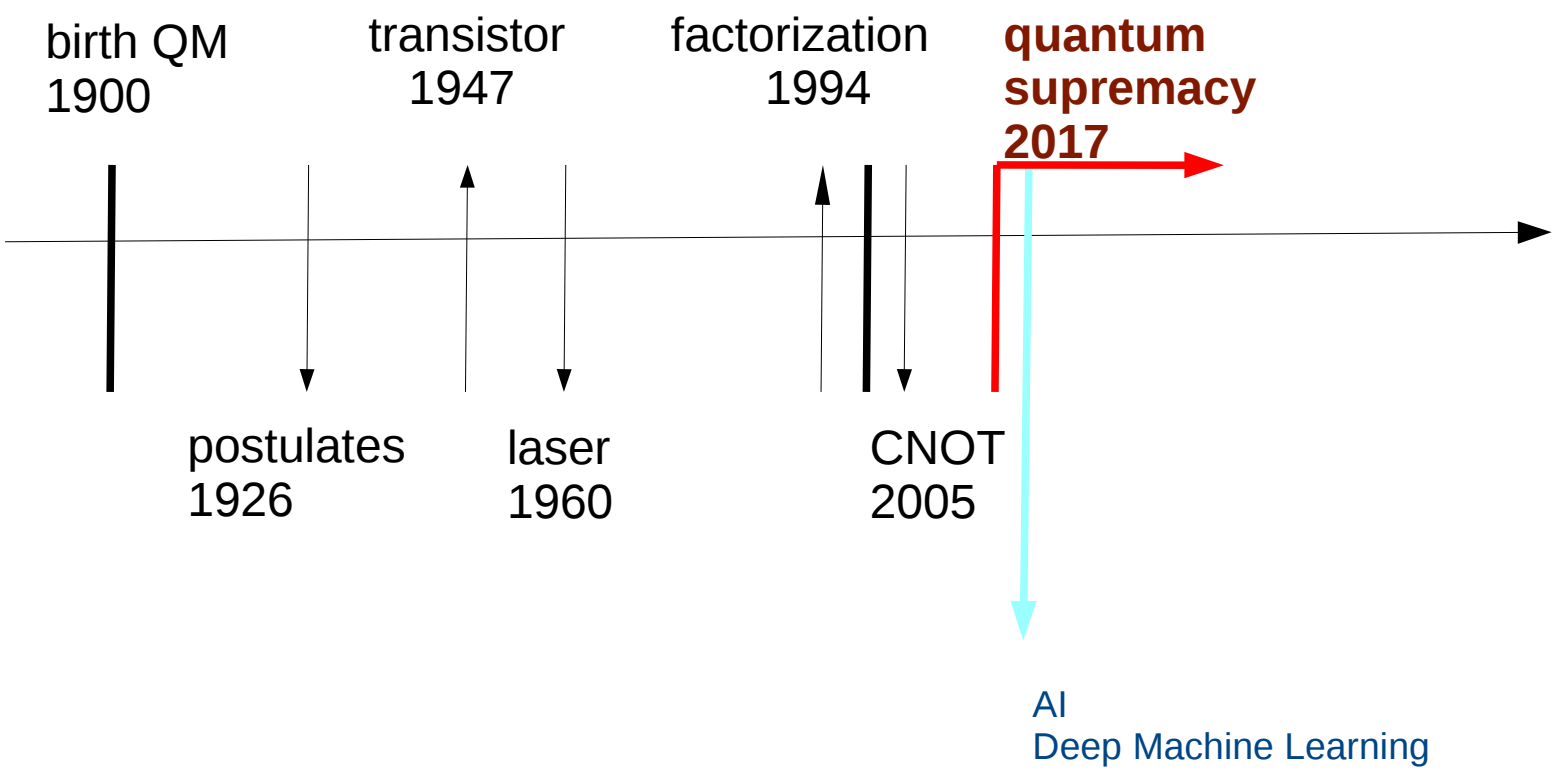
Micius satellite



48 nodes

SECOND
QUANTUM REVOLUTION

Second QUANTUM REVOLUTION

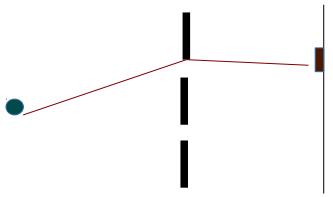


QUANTUM POSTULATES

- Information $|\psi\rangle \in \mathcal{H}$
- Observables $O = \sum_o o\, E_o \qquad E_o = |o\rangle\langle o|$
- Measurement $P_{O,|\psi\rangle}(o) = \| E_o |\psi\rangle \|^2$
- Evolution $U = U^+$

Superposition

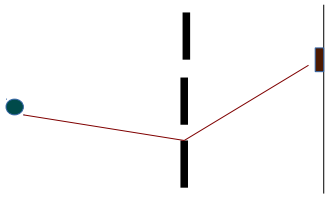
The information on a system may be on a ***superposition*** of various possibilities



$$|\psi_1\rangle$$

Superposition

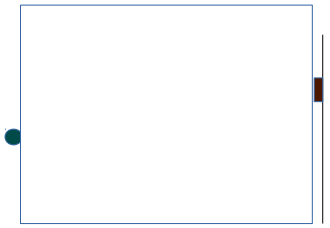
The information on a system may be on a ***superposition*** of various possibilities



$$|\psi_2\rangle$$

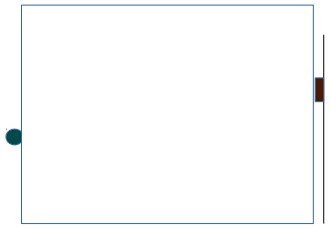
Superposition

The information on a system may be on a ***superposition*** of various possibilities



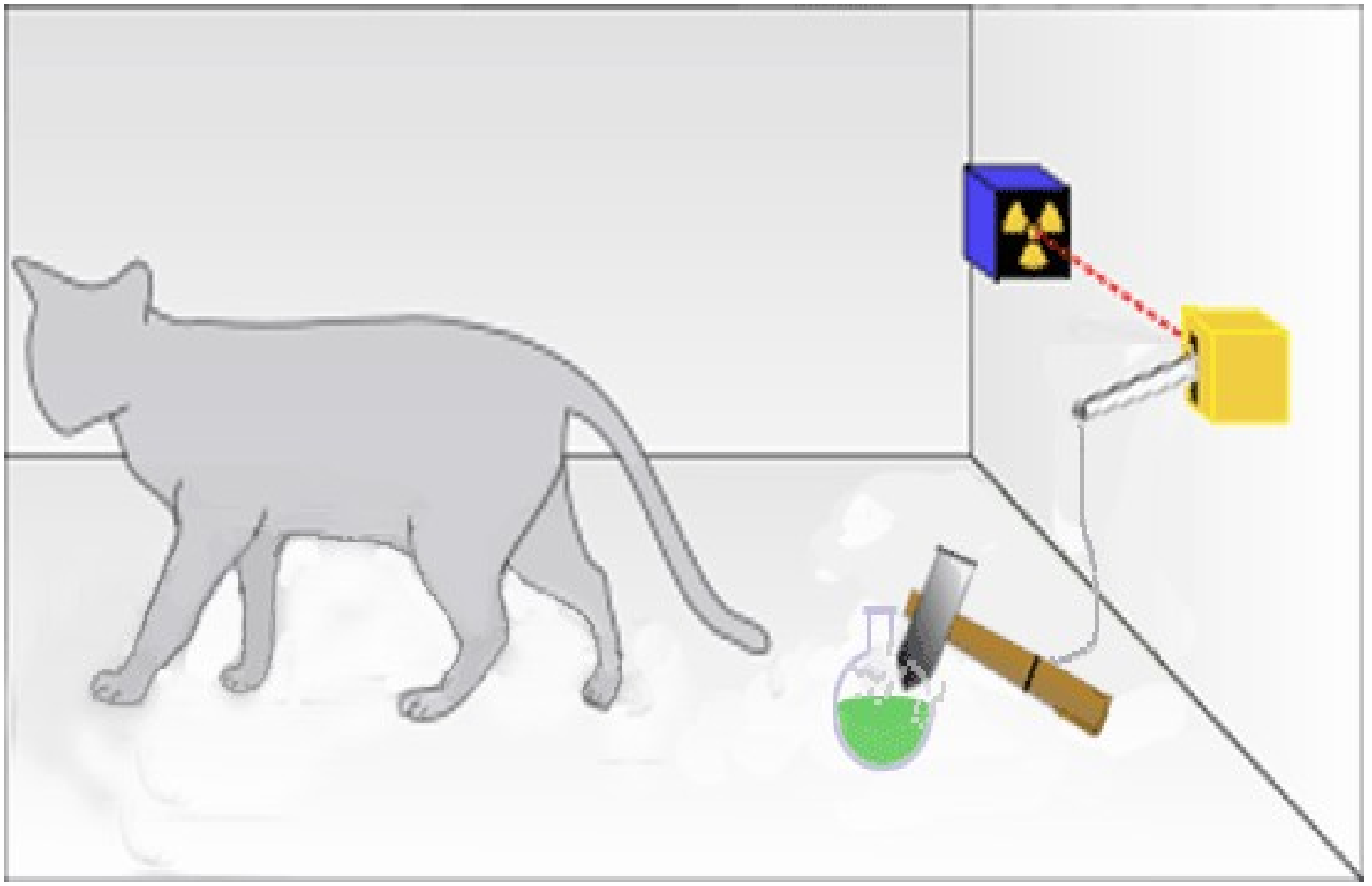
Superposition

The information on a system may be on a ***superposition*** of various possibilities

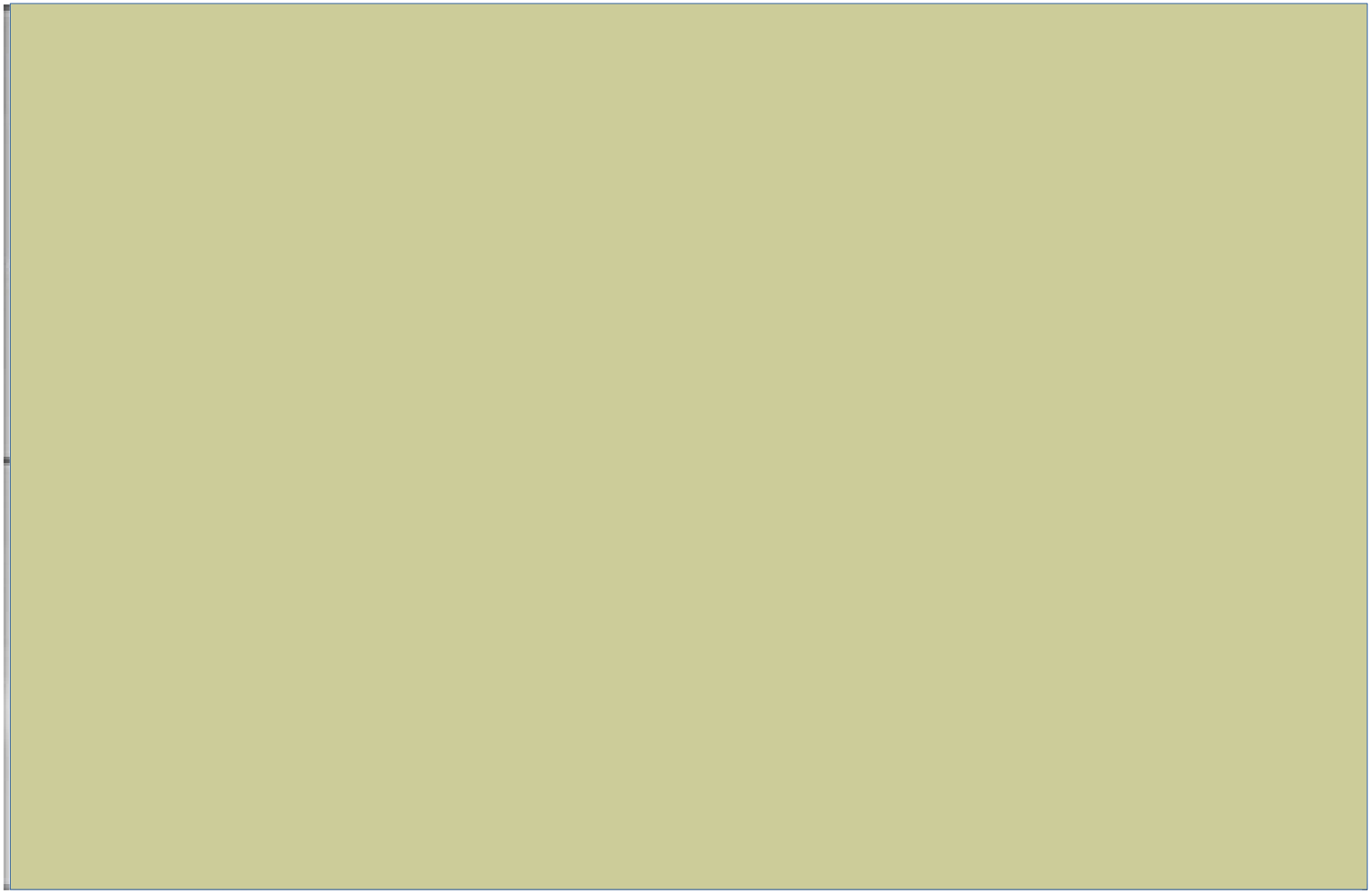


$$|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$$

Schrödinger's cat



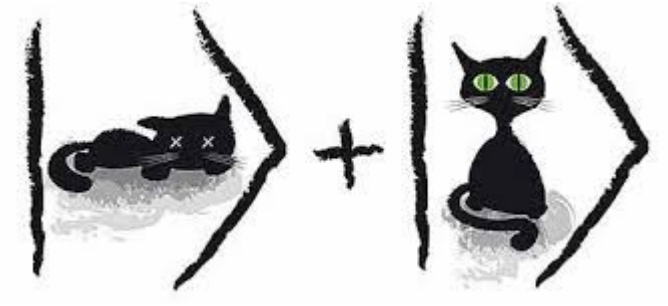
Schrödinger's cat



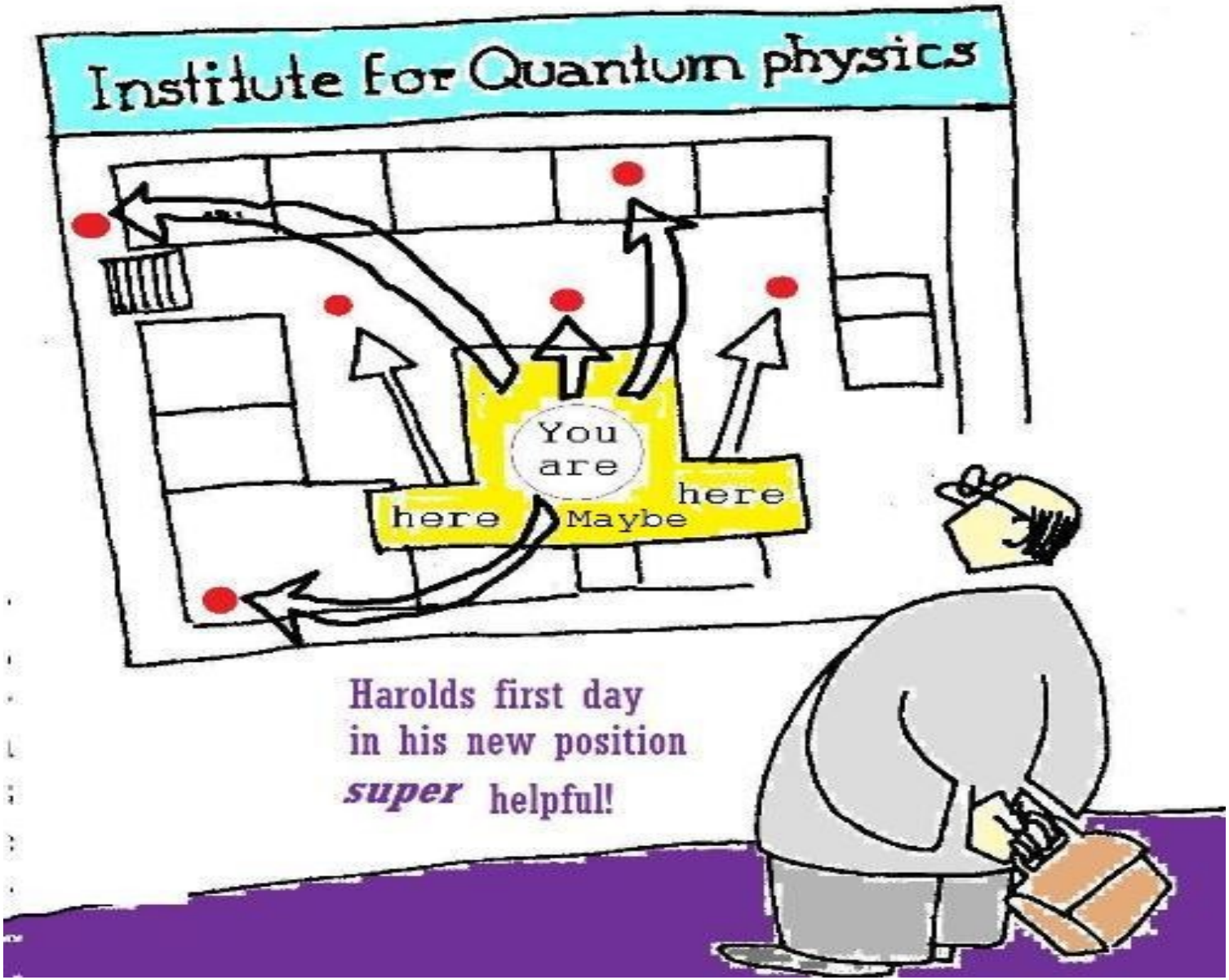
Schrödinger's cat

$$|cat\rangle = |alive\rangle + |dead\rangle$$

Schrödinger's cat kills your prejudices



'bout your cat, Mr. Schrödinger—I have good news and bad news."


Institute for Quantum physics
You are here
here
Maybe here
Harolds first day
in his new position
super helpful!

No cloning (Wooters-Zurek, 1982)

$$U_{xerox}|0\rangle|a\rangle=|0\rangle|0\rangle$$

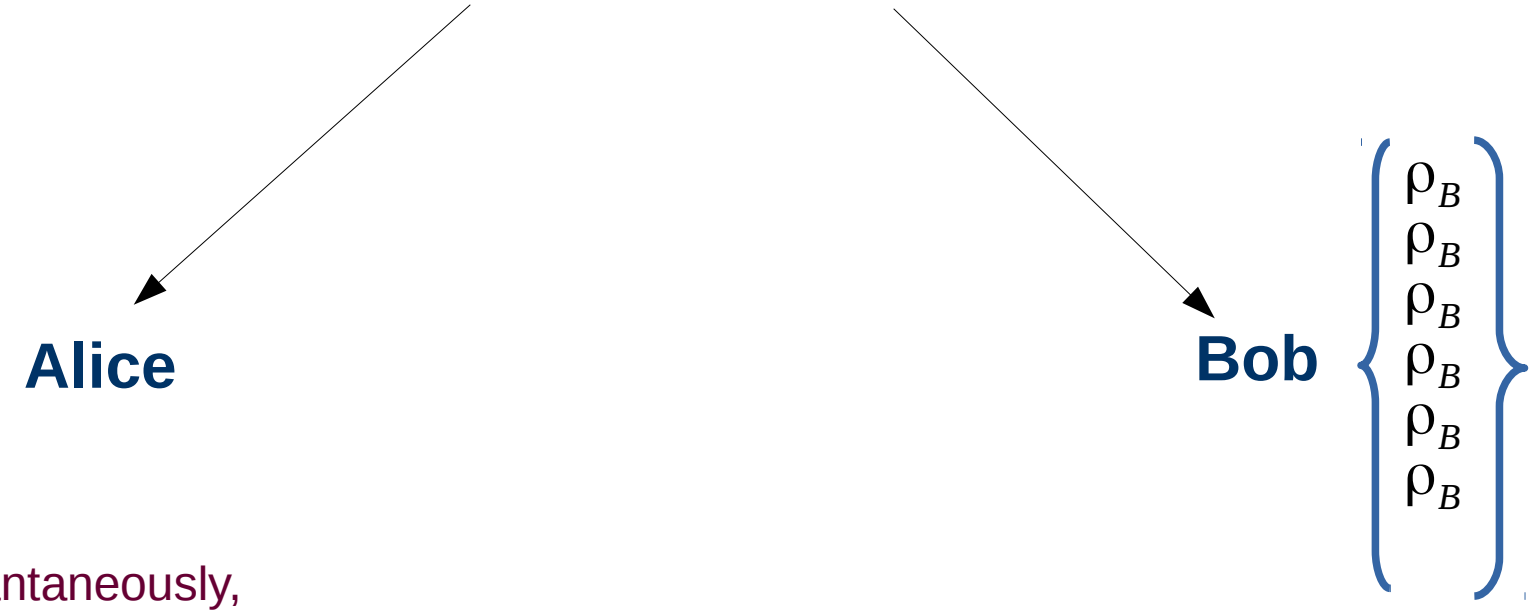
$$U_{xerox}|1\rangle|a\rangle=|1\rangle|1\rangle$$

$$U_{xerox}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|a\rangle=\frac{1}{\sqrt{2}}|0\rangle|0\rangle+\frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

$$\neq\frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)$$

No cloning vs superluminical communication

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$



Instantaneously,

A either measures of not, B always measures

If A measures, B finds the same state always

If A does not measure, B finds a mixed state

Let's use quantum superposition to codify information

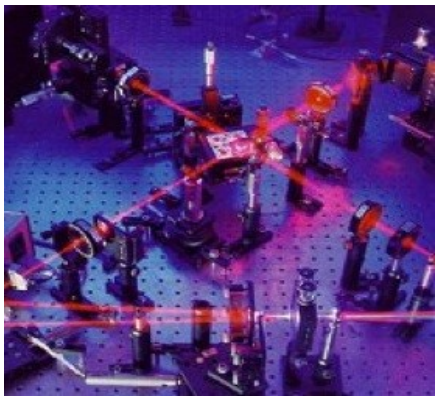
We can codify arbitrary superpositions of logical bits: QUBIT

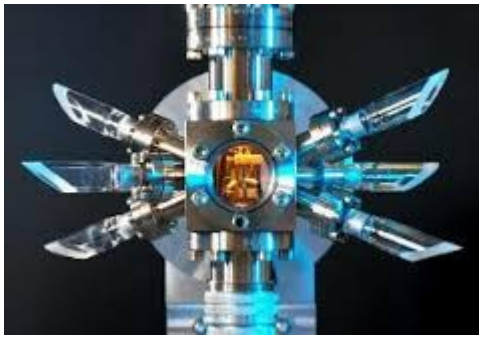
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

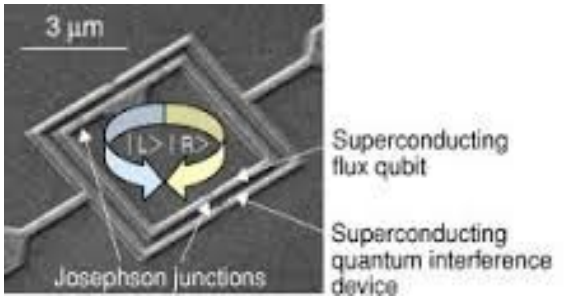
Physical implementation of qubits

Quantum Cryptography

Quantum Computation







Photons:
H-V polarization
Time bins

Trapped ions:
ground-excited energy

Superconducting curents:
Left-right rotation

Massive superpositions for computation

Many qubits on a single quantum register

$$|\psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$

n=3 qubits we may process 8 superposicions

Parallel processing = Massive parallel computation

Example: add simultaneously 1 to (0, 2, 6)

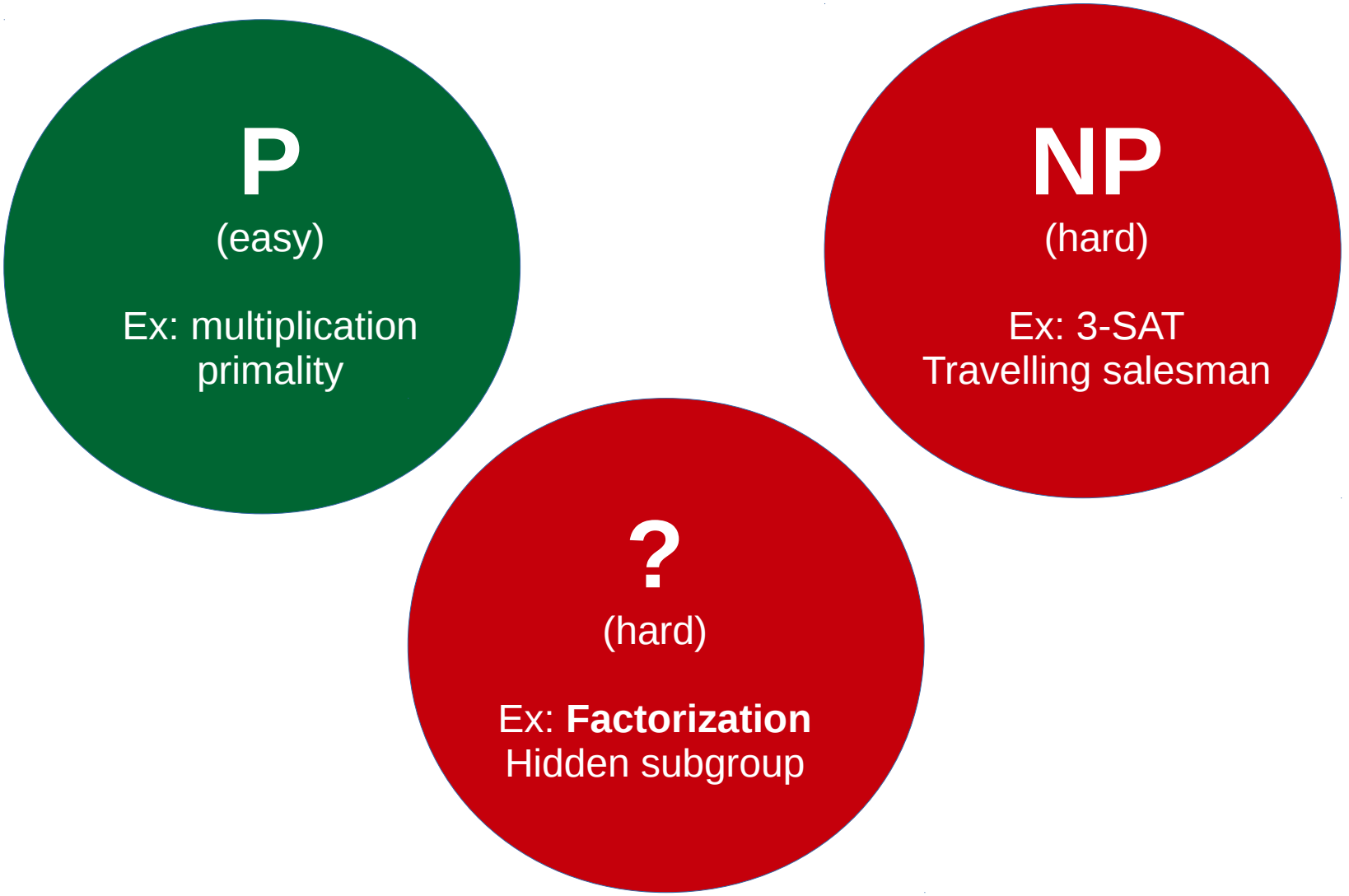
$$|\psi\rangle = \underbrace{|000\rangle}_{0} + \underbrace{|010\rangle}_{2} + \underbrace{|110\rangle}_{6}$$

We can add 1 in a single laser pulse!!

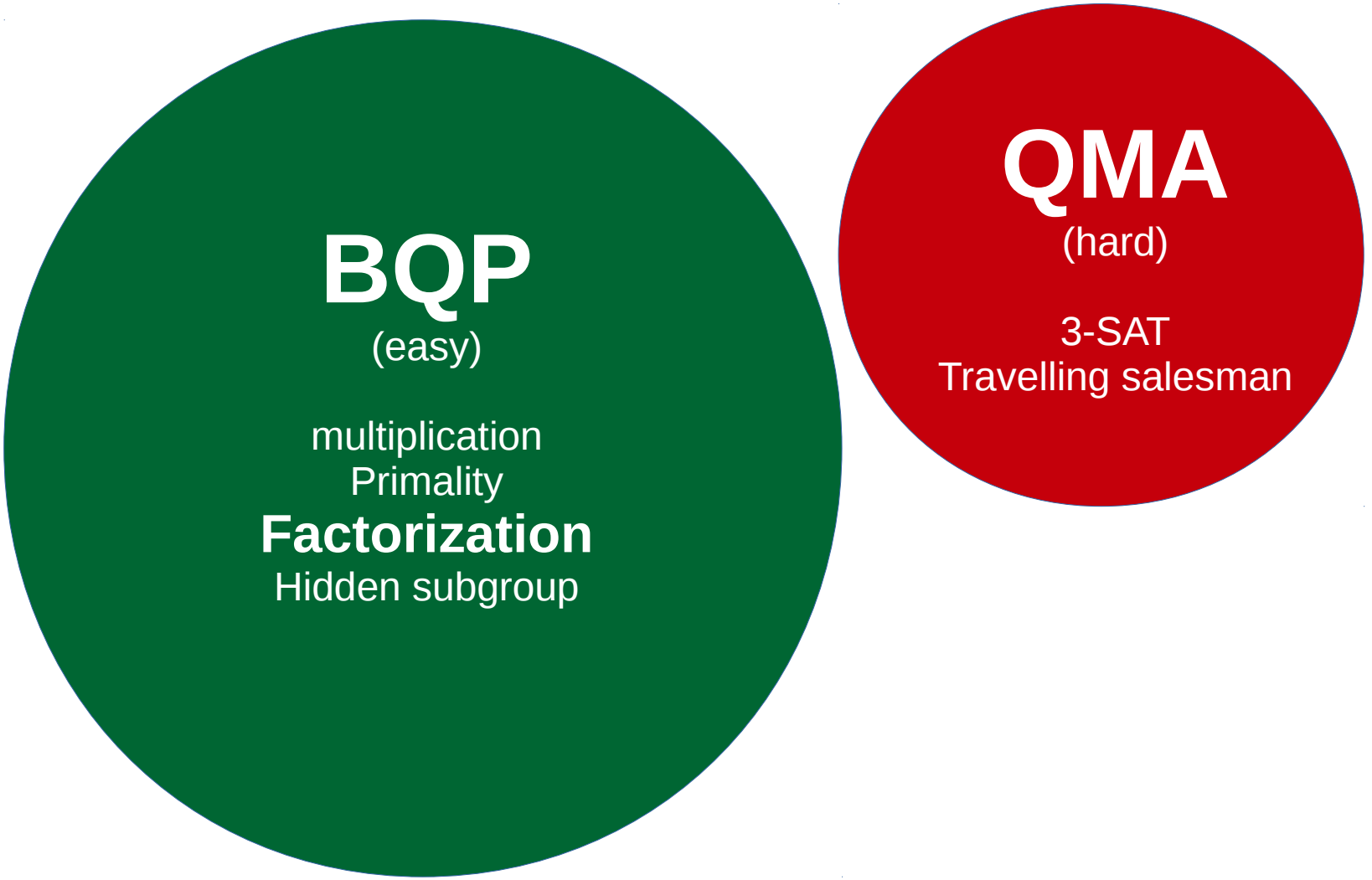
$$U_{+1}|\psi\rangle = U_{+1}|000\rangle + U_{+1}|010\rangle + U_{+1}|110\rangle$$

$$= \underbrace{|001\rangle}_{1} + \underbrace{|011\rangle}_{3} + \underbrace{|111\rangle}_{7}$$

Which problems can be solved with a Classical Computer?



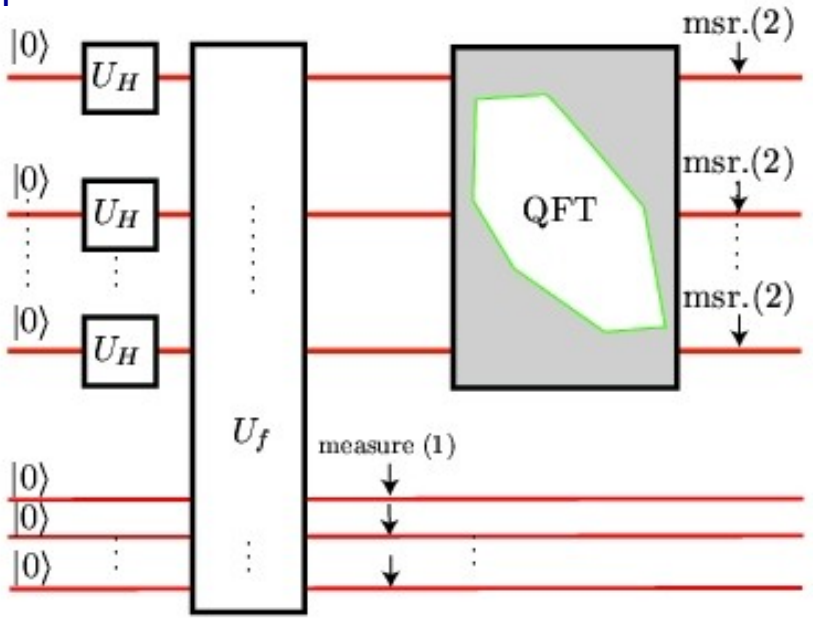
Which problems can be solved with a Quantum Computer?

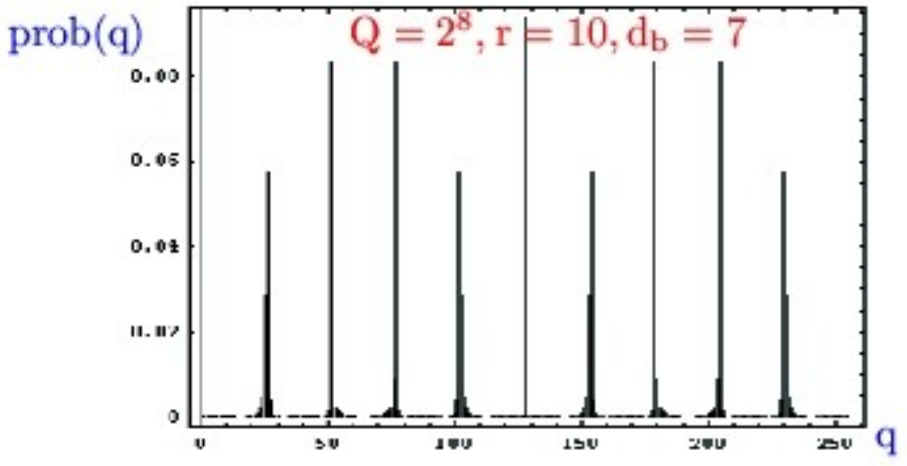


Shor's algorithm (1994)

Factorization = Find a period = Hidden subgroup problem
Key fact: efficient Quantum Fourier Transform

$$P(q) = \frac{1}{QB}\left|\sum_{k=0}^{B-1} e^{iqr\,2\pi/Q}\right|^2$$



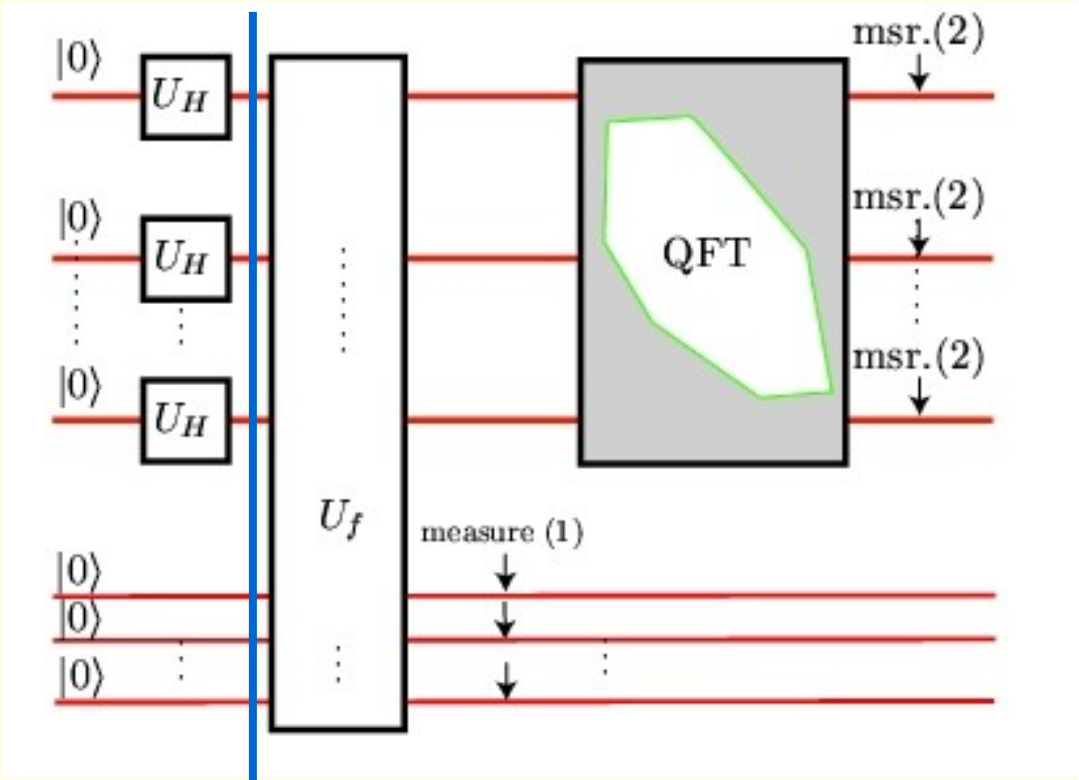


Read r

q= m Q/r

1. **Inicialize the register**

$$|\psi_1\rangle = |00..0\rangle_{target}\ |00..0\rangle_{ancillae}$$

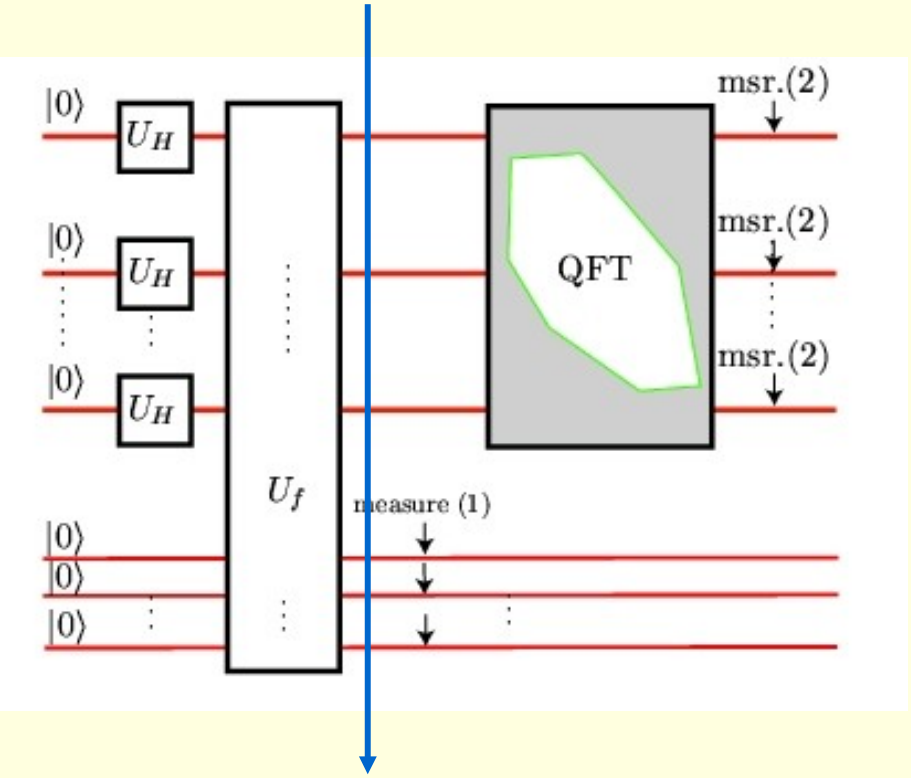


2. **Superpose all numbers**

$$U_H\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

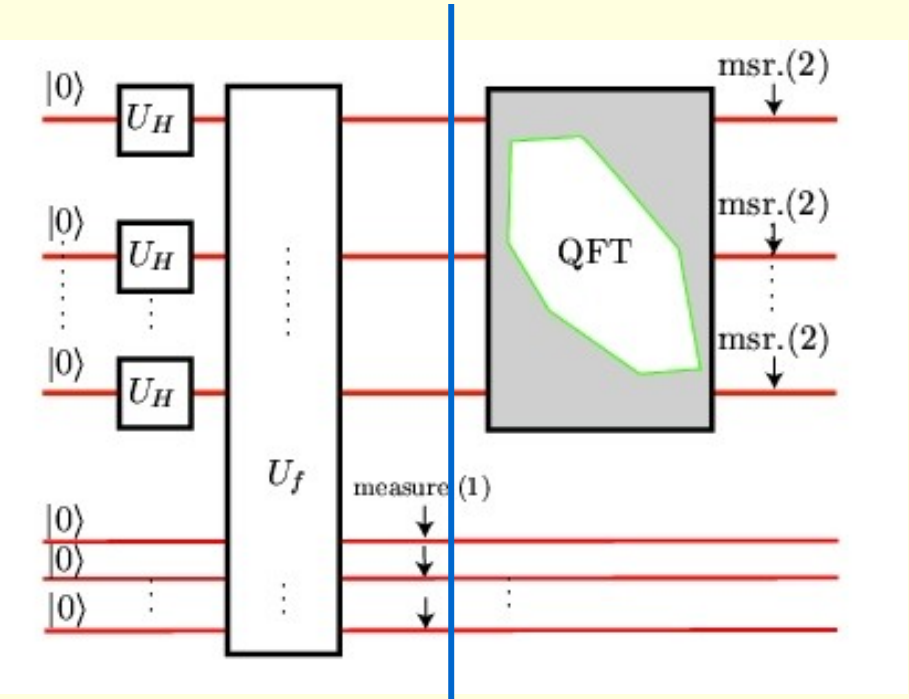
$$|\psi_2\rangle = U_H^{(1)} \otimes \ldots \otimes U_H^{(n)}\ |00..0\rangle\,|00..0\rangle = \sum_{x=0}^{2^n-1} |x\rangle\,|00..0\rangle$$

3. Parallel modular exponenciation



$$|\psi_3\rangle = U_f\,|\psi_2\rangle = \frac{1}{Q}\sum_{x=0}^{2^n-1}|x\rangle\,|a^x \bmod(N)\rangle$$

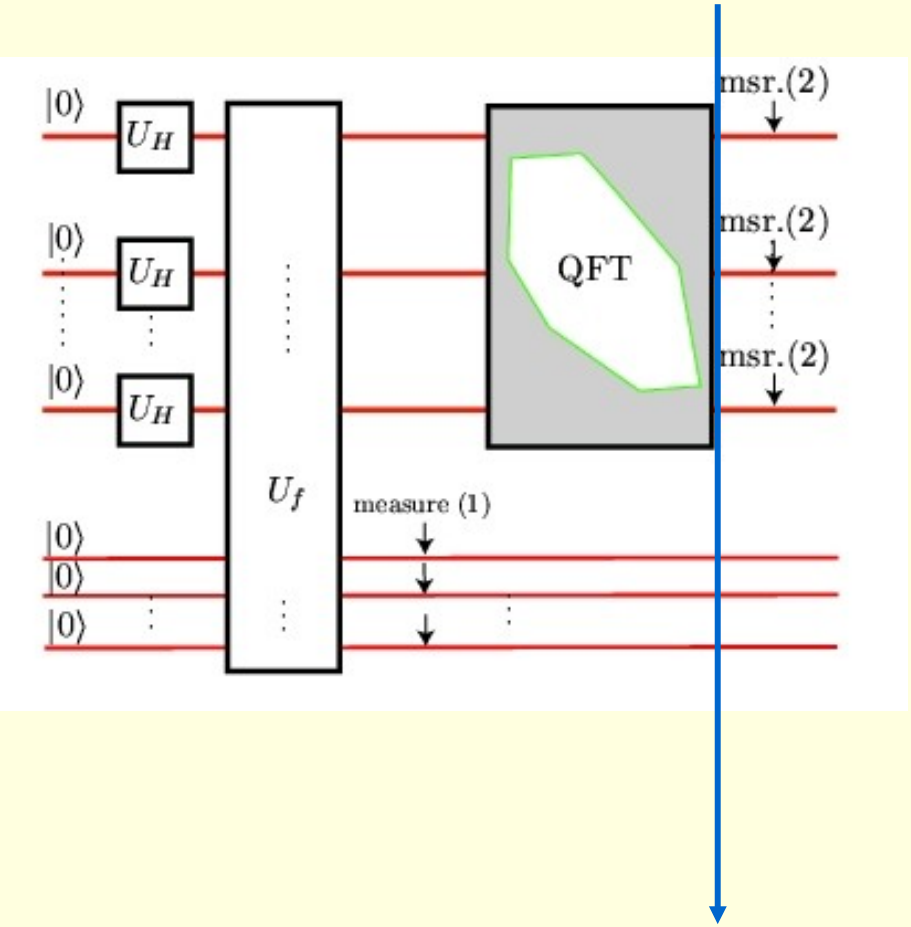
4. Measure ancillae



$$|\psi_3\rangle = U_f\,|\psi_2\rangle = \frac{1}{Q}\sum_{x=0}^{2^n-1} |\,x\rangle\,|\,a^x \bmod(N)\rangle$$

$$|\psi_4\rangle = \frac{1}{B}\sum_{k=0}^{B-1} |\,d_b + kr\rangle\,|\,b\rangle$$

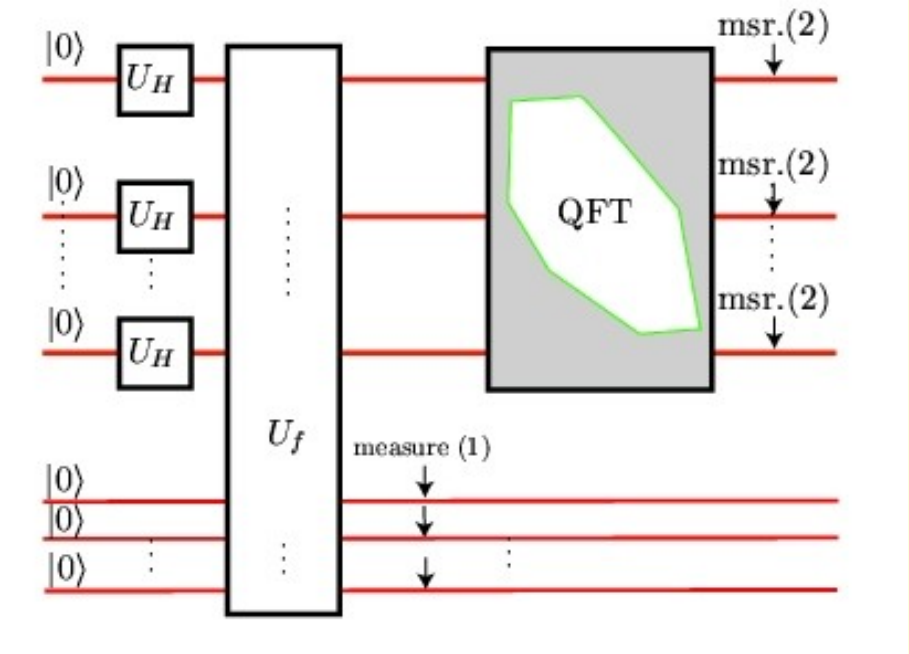
5. Quantum Fourier Transform

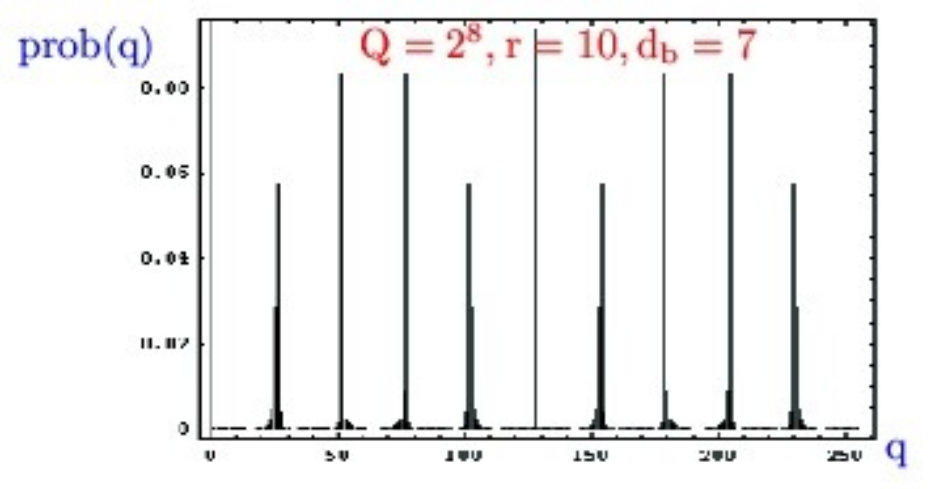


$$|\psi_5\rangle = \frac{1}{\sqrt{QB}} \sum_q \sum_k e^{iq\,2\pi(d_b + kr)} \,|q\rangle\,|b\rangle$$

6. Target shows period

$$P(q) = \frac{1}{QB}\left|\sum_{k=0}^{B-1} e^{iqr\,2\pi/Q}\right|^2$$





Picked at

q= m Q/r **read r**

Factorization (QFT)

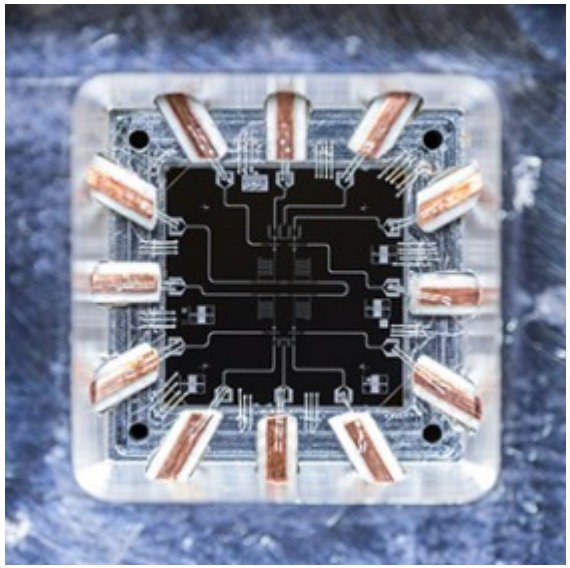
Classical Computer

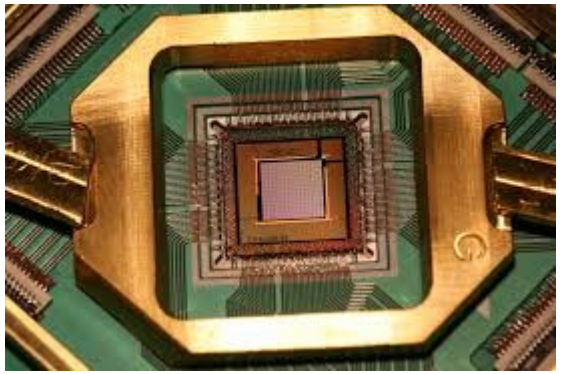
$$e^{\left(\frac{64}{9}\right)^{1/3} n^{1/3} (\log n)^{2/3}}$$

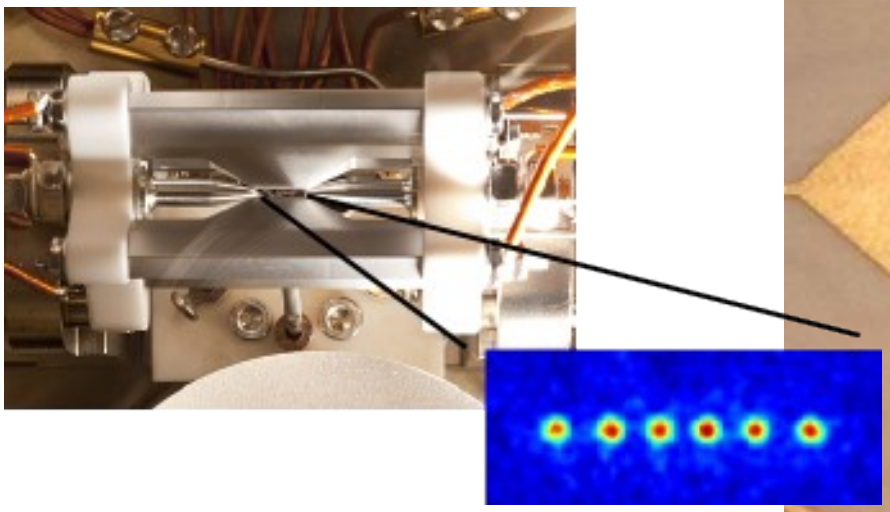
Quantum Computer

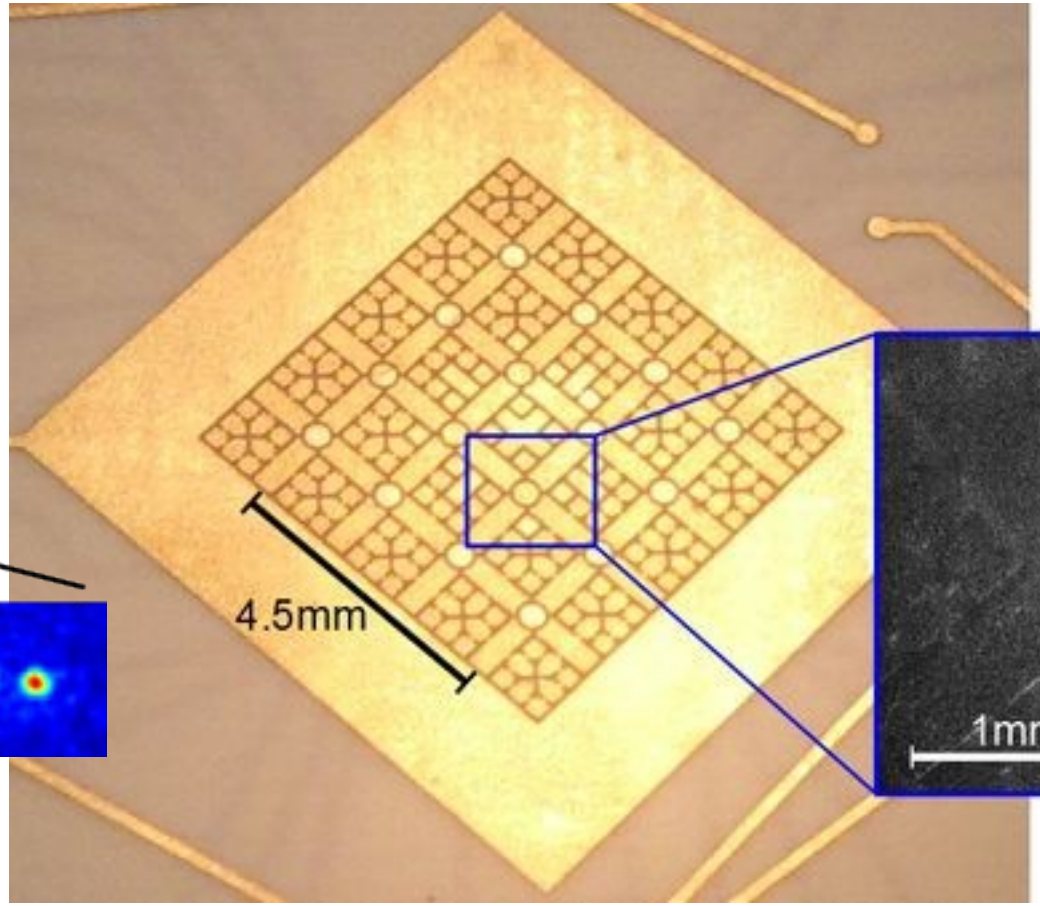
$$n^2 (\log n)(\log(\log n))$$

Shor's algorithm is exponentially faster








4.5mm
1mm

Quantum Gates

Martinis 9 qubit experiment
Martinis 49 Quantum Supremacy proposal
Monz 5 qubit full QFT
Blatt 16 qubit Mermin inequalities

Anealing

DWAVE

$$H = (1-s)\sum \sigma_i^x + s\,H_P$$

$$H_P = \sum_{ij} \alpha_{ij}\,\sigma_i^z\,\sigma_j^z$$

α_{ij} nearest neighbor

Sooner than later

A Quantum Computer will factor larger numbers efficiently!!!

RSA classical cryptography will be broken

Are we ready for that?

QUANTUM CRYPTOGRAPHY

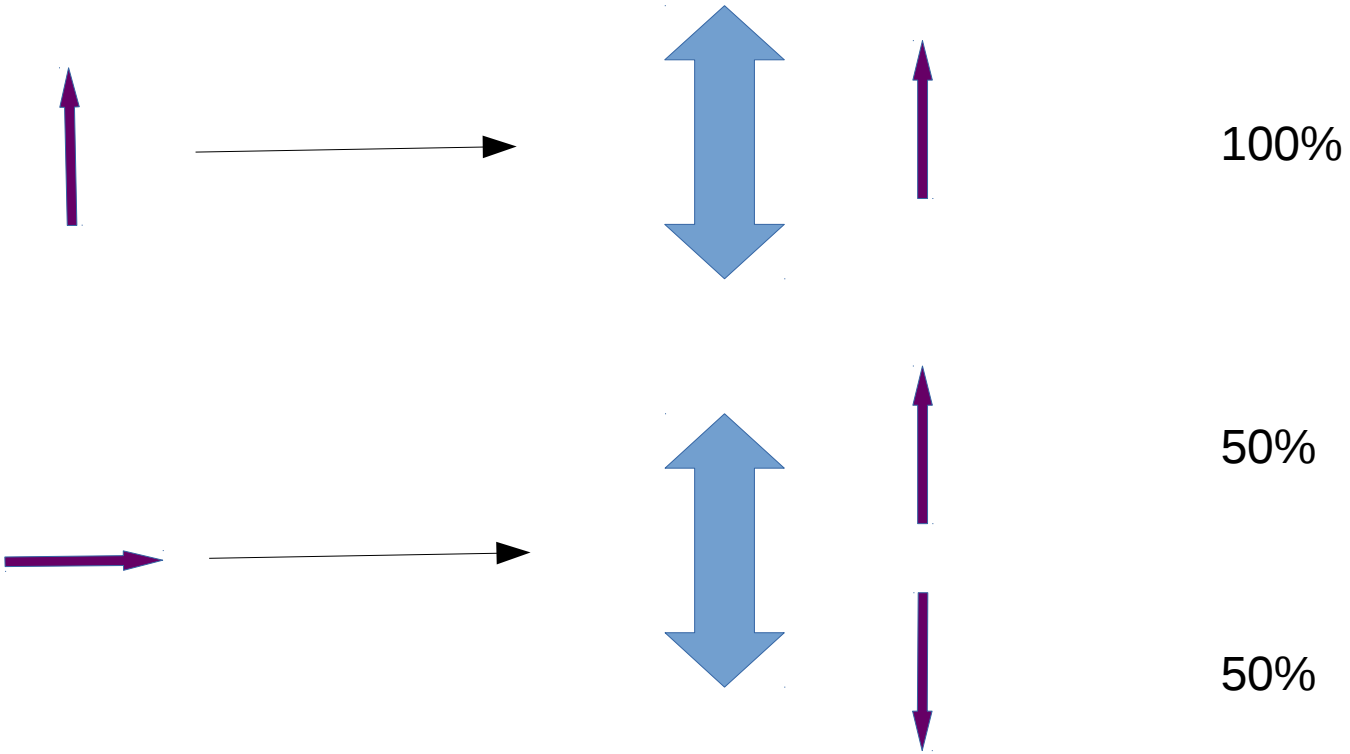
Key idea

When me measure a state, we **alter** it

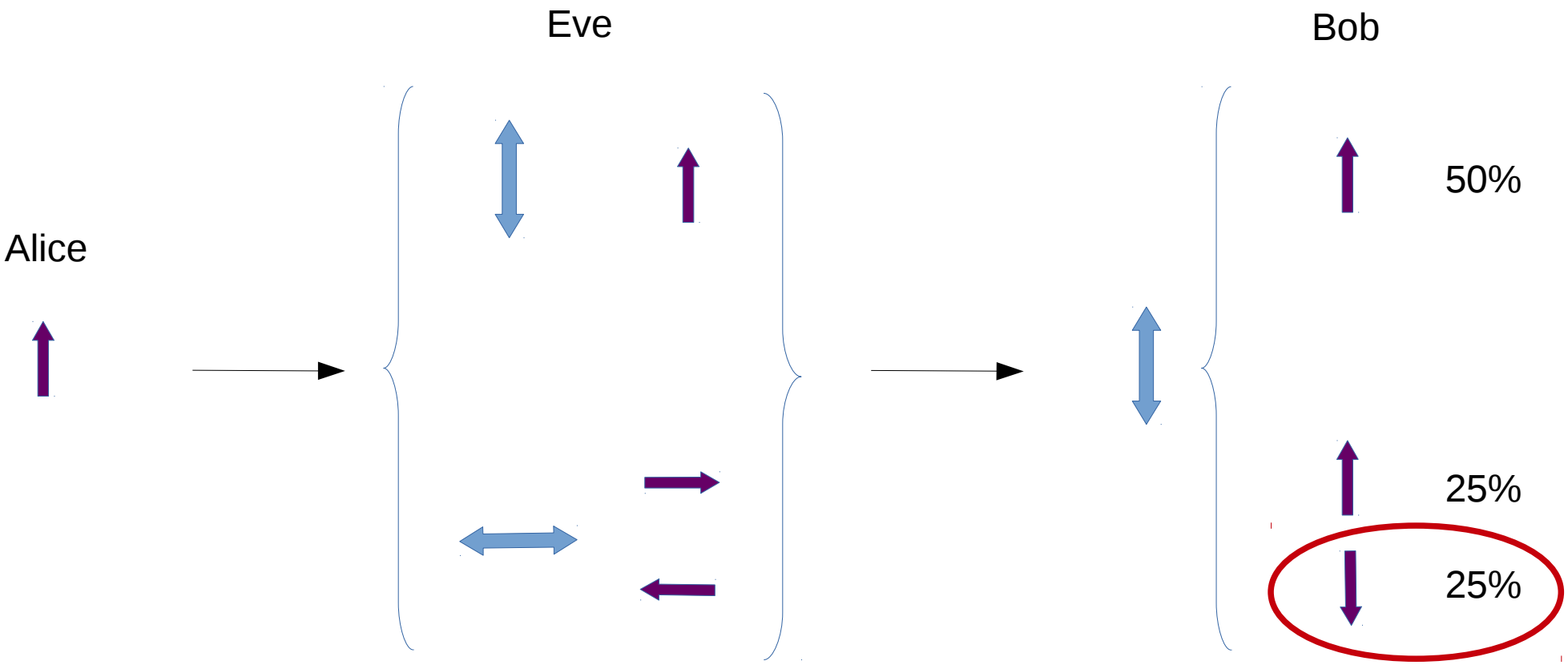
The process of observing a state **modifies** it in an uncontrolable way

The presence of Eve can be uncovered!

BB84

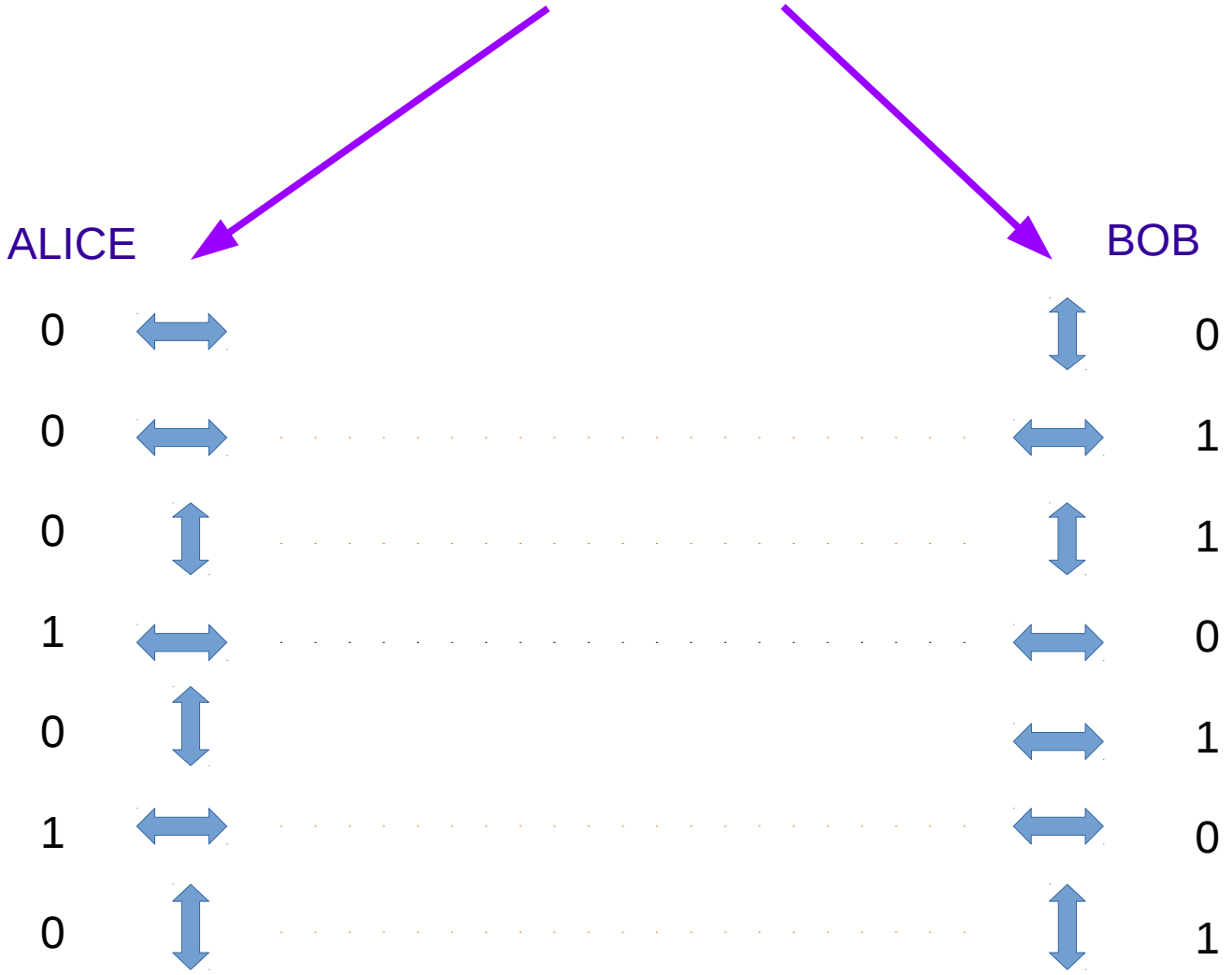


BB84: man in the middle attack



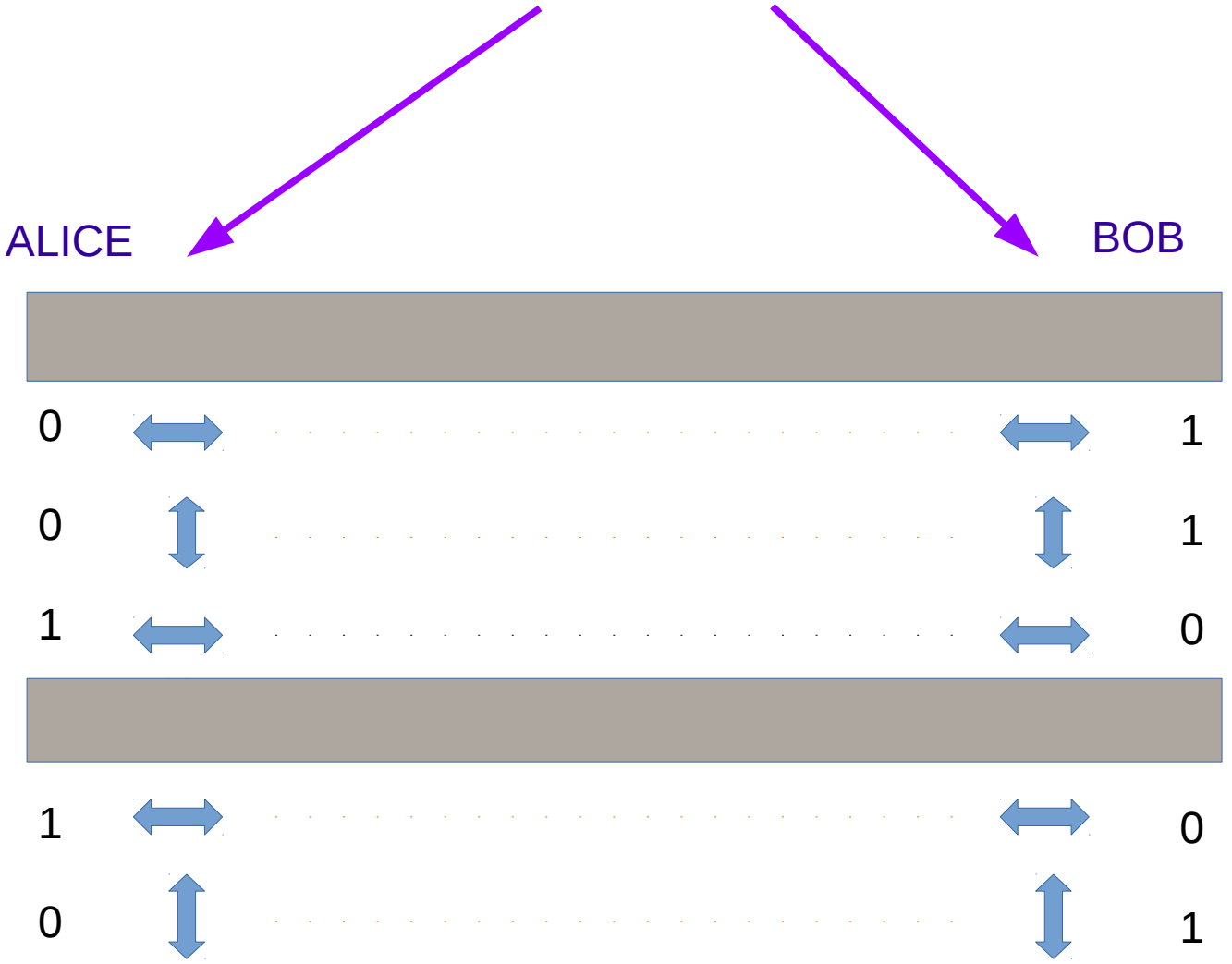
EKERT91

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01-10\rangle$$



EKERT91

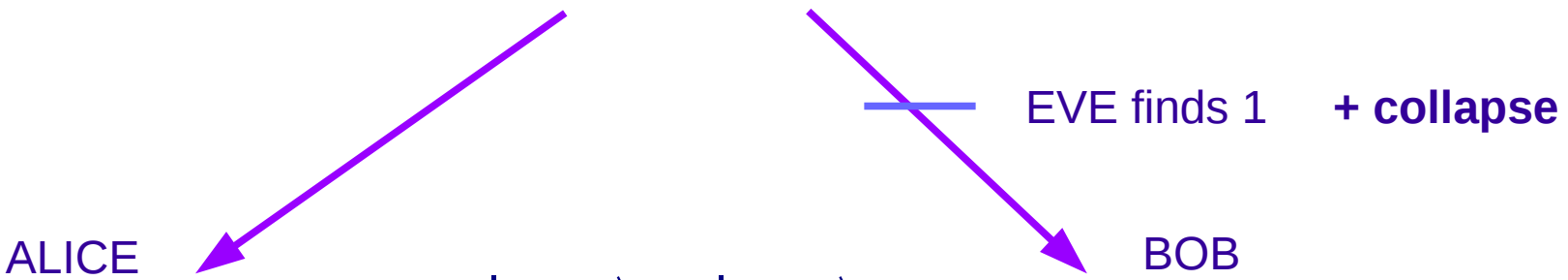
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01-10\rangle$$



ALICE and BOB share a secret key

EKERT91

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01-10\rangle$$

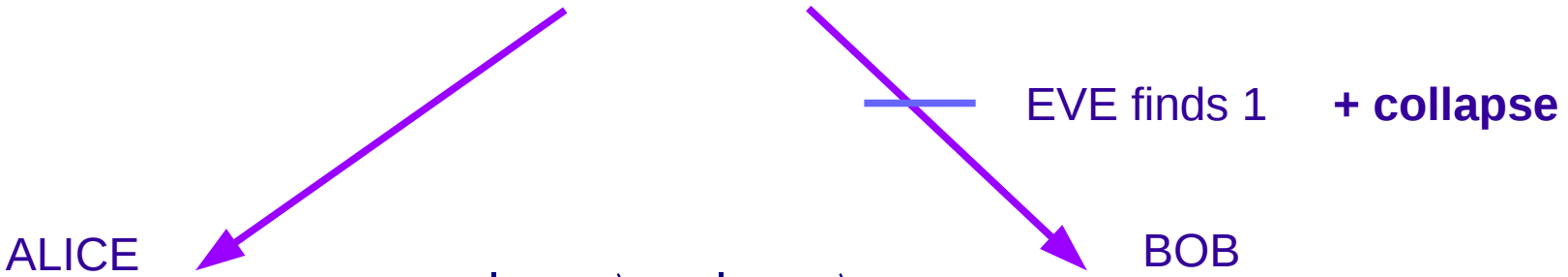


$$|\psi'\rangle = |01\rangle$$

How to detect EVE?

EKERT91

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01-10\rangle$$



$$|\psi'\rangle = |01\rangle$$

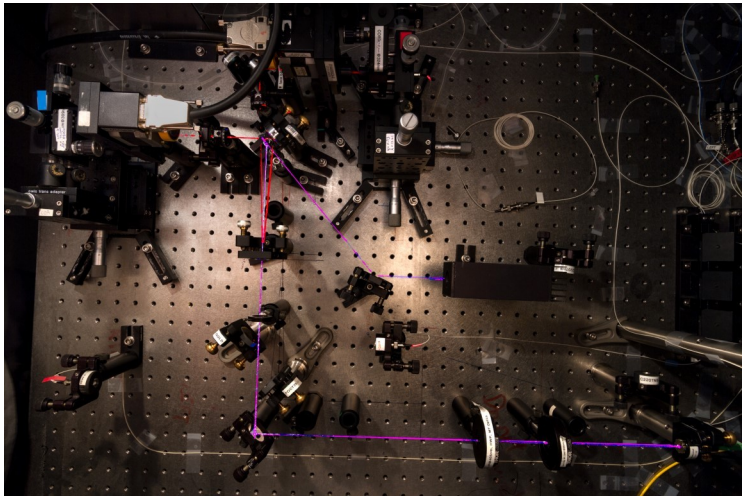
Alice and Bob measure Bell inequalities

$$\langle ab + ab' + a'b - a'b' \rangle_{|\psi^-\rangle} \sim 2\sqrt{2}$$

$$\langle ab + ab' + a'b - a'b' \rangle_{|\psi'\rangle} \leq 2$$

Violation of Bell Inequalities are no longer a proof of QM
but an instrument for cryptography
Entanglement is a resource for Ekert 91

Best check of quantum weirdness (2015)



$2\sqrt{2}$ ~2.82843

Hou Shun et al. 2015 experiment (NUS): 2.82759 ± 0.00051

Quantum crryptographic protocoles can be proven unbreakable

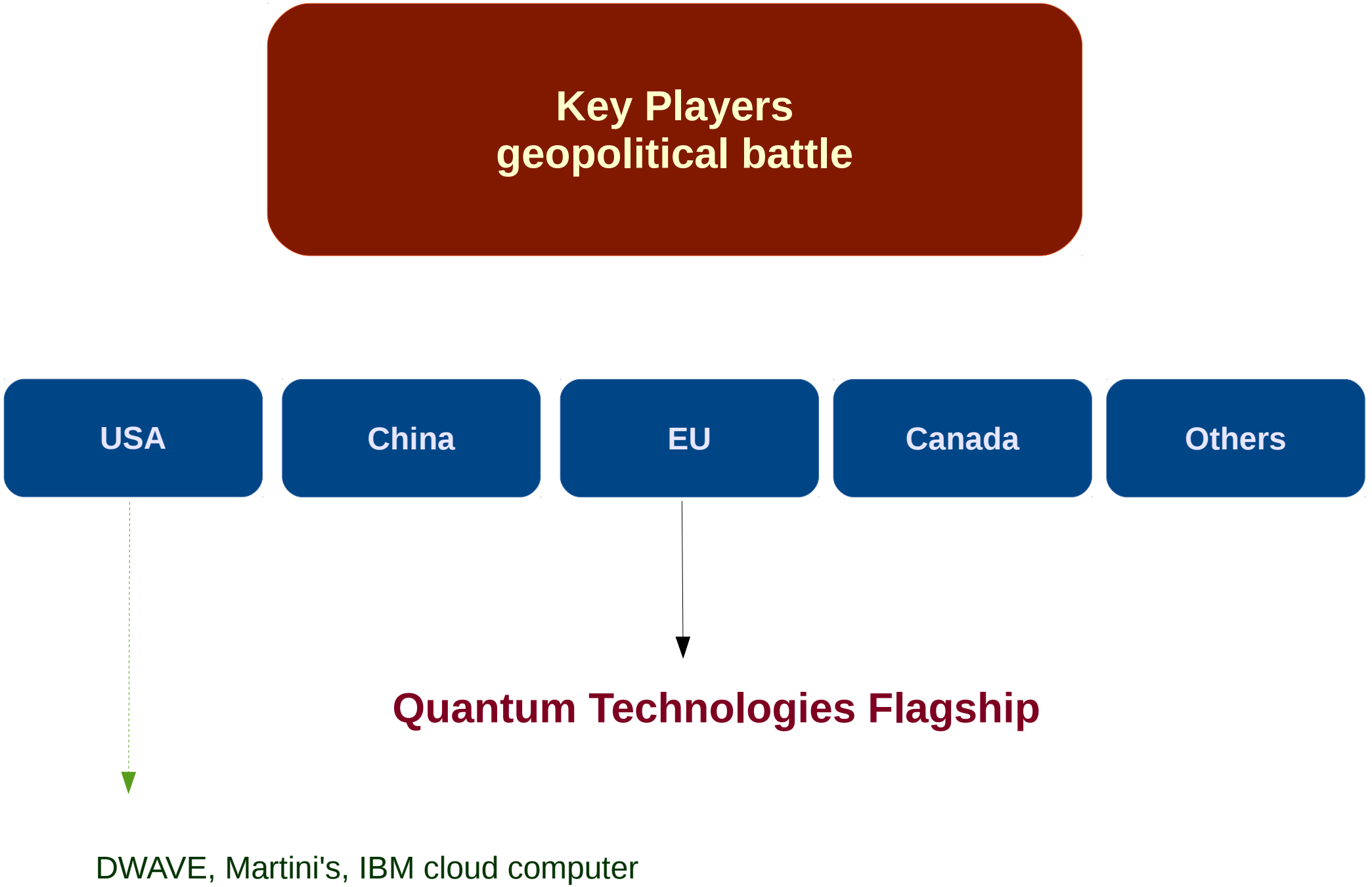
(even if Eve is more non-local than quantum)

Device independent certifiable security!

Post-Quantum cryptography

Hardware vs software security

POLITICS + BUSINESS


Key Players
geopolitical battle
USA
China
EU
Canada
Others
Quantum Technologies Flagship
DWAVE, Martini's, IBM cloud computer

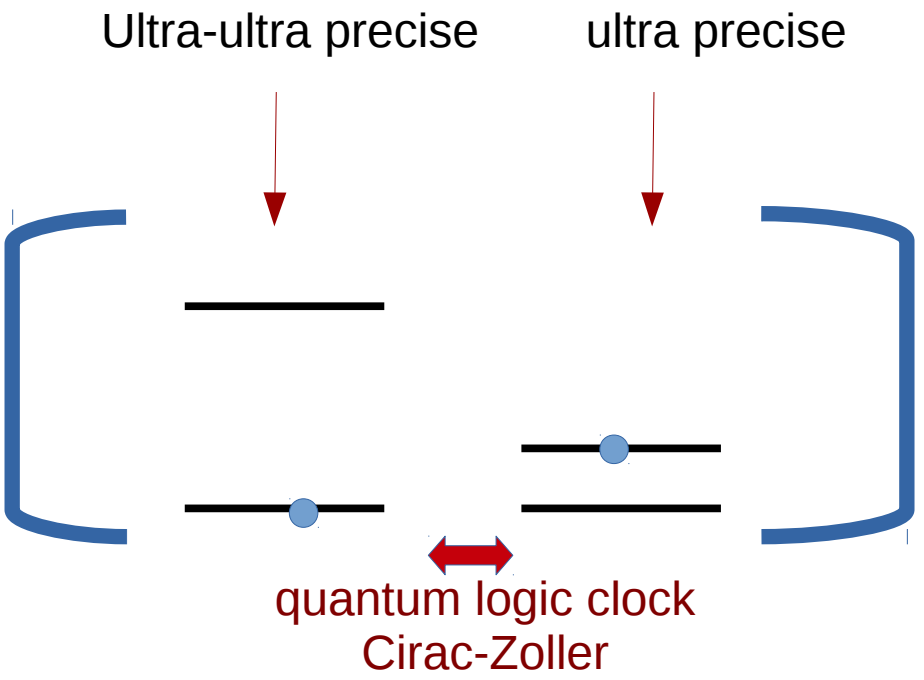
Quantum Technologies

5 Pillars

- Computation
- Communication
- Sensors
- Simulation
- Algorithms

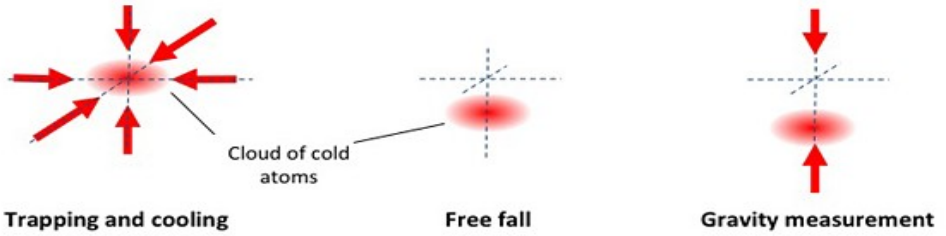
New Quantum Clocks

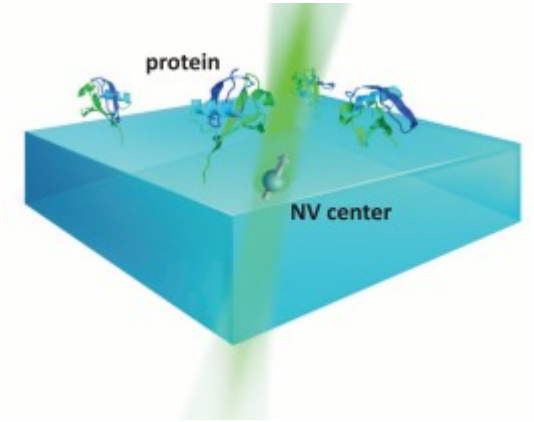
Precision 1 part in 10^{18}



Gravimeter

Accelerometer microGal





Diamond

Add a Nitrogent Vacancy center

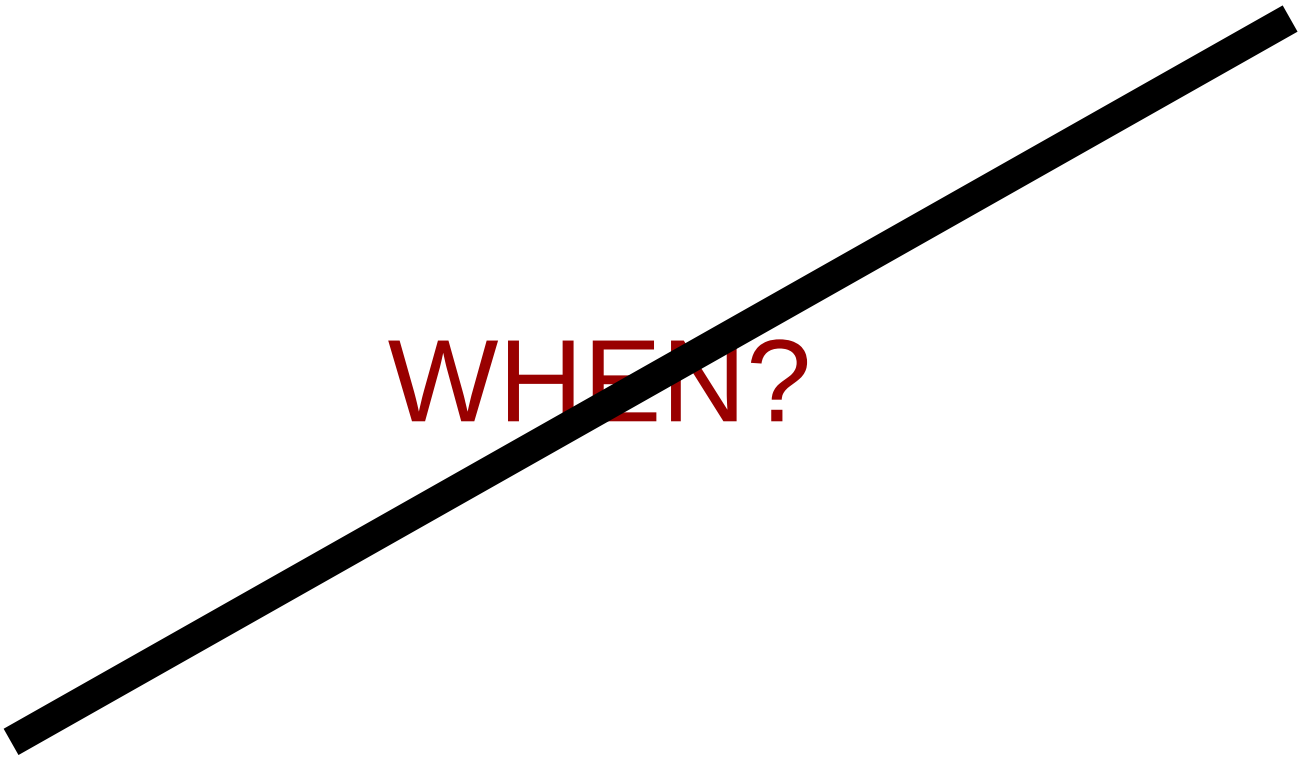
Bring a molecule to the surface

Read its structure with a single atom!!!!

BIG QUESTION

WHEN?

Quantum Supremacy: Martini's 2017
DWAVE2 2048 qubits
QFT Innsbruck


WHEN?

WHO?

Who will have the tool to break classical cryptography?

Which nation?

Which corporation?

Open research / Proprietary research

Which laws will be passed?

What political agenda will develop in the near future?

CONCLUSION

Business

New (quantum&risruptive) generation of techonology
New advanced skills will be needed: fight for deep talent
Radical new ventures

Politics

Serious world competition
(Some parallelism with the dawn of atomic weapons)
Quantum research will provide some countries with a huge political advantage
Quantum Leverage

THANKS !!!!

Are we prepared for the Quantum Future?