Quantum Disruption

IFAE, February 2018

José Ignacio LATORRE
Univ. Barcelona / National Univ. Singapore
Quantic@BSC-UB

UNIVERSITAT DE BARCELONA

NUS National University of Singapore

CENTRO DE CIENCIAS DE BENASQUE PEDRO PASCUAL

| Entanglement Partners_ >

IN THE NEWS

(hype?)

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

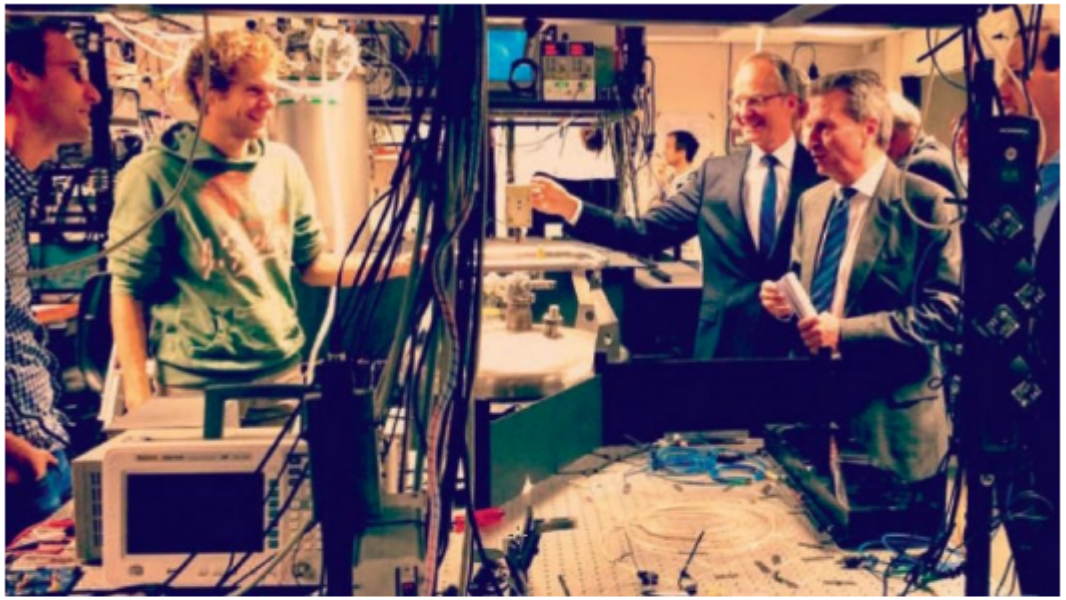
Enlarge / Hillary Clinton.

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

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

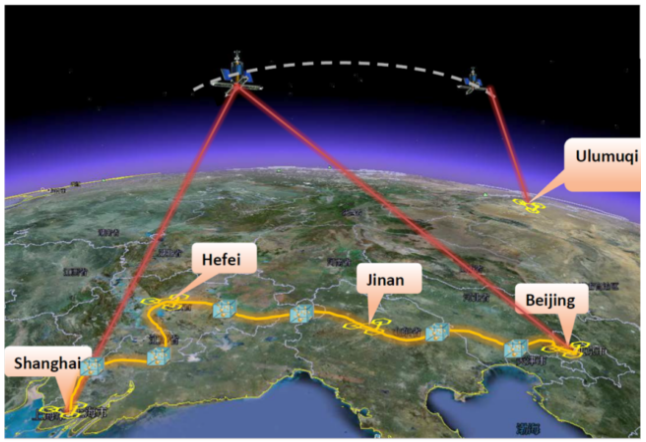
Call 02/2018

China

NATIONAL LABORATORY FOR QUANTUM INFORMATION SCIENCES

The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.

CNTV



48 trusted nodes

Micius satellite
Tibet, 1200 km apart
Austria-China (9/2017)

Wolfsburg/Hanover, 20 March 2017

Research project successful: Volkswagen IT experts use quantum computing for traffic flow optimization

- **CeBIT 2017: Volkswagen announces cooperation with leading quantum computing company D-Wave Systems**
- **First research project successful: travel times of 10,000 taxis in mega-metropolis of Beijing significantly reduced**

Dr. Christian Seidel, Senior Data Scientist from Volkswagen Group IT's Data Lab in Munich, Robert „Bo" Ewald, President D-Wave International, Dr. Martin Hofmann, CIO of Volkswagen Group, Dr. Fl...

The Volkswagen Group is the world's first automaker to intensively test the use of quantum computers. Volkswagen is cooperating with leading quantum computing company specialist D-Wave Systems. At CeBIT 2017, the two companies today announced their cooperation. In a first research project, IT experts from Volkswagen have already successfully developed and tested a traffic flow optimization algorithm on a D-Wave quantum computer.

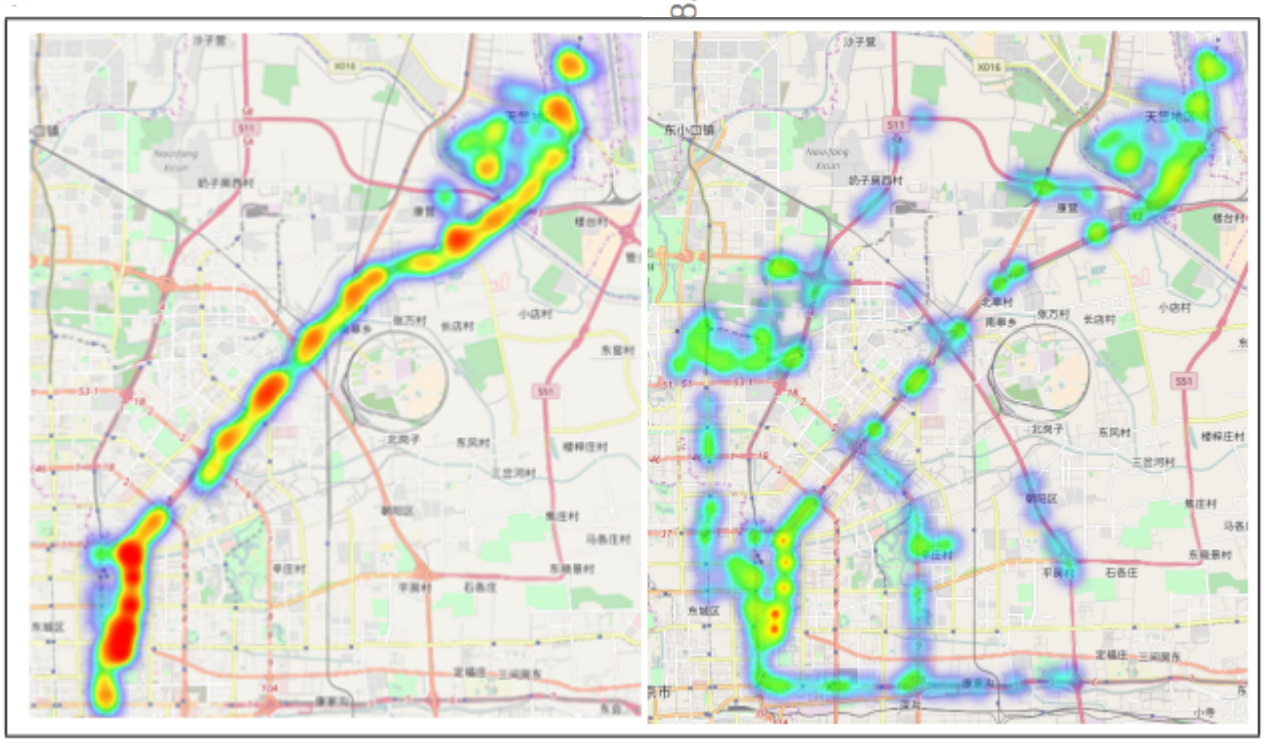
Traffic flow optimization using a quantum annealer

Florian Neukart*[1], David Von Dollen[1], Gabriele Compostella[2], Christian Seidel[2], Sheir Yarkoni[3], and Bob Parney[3]

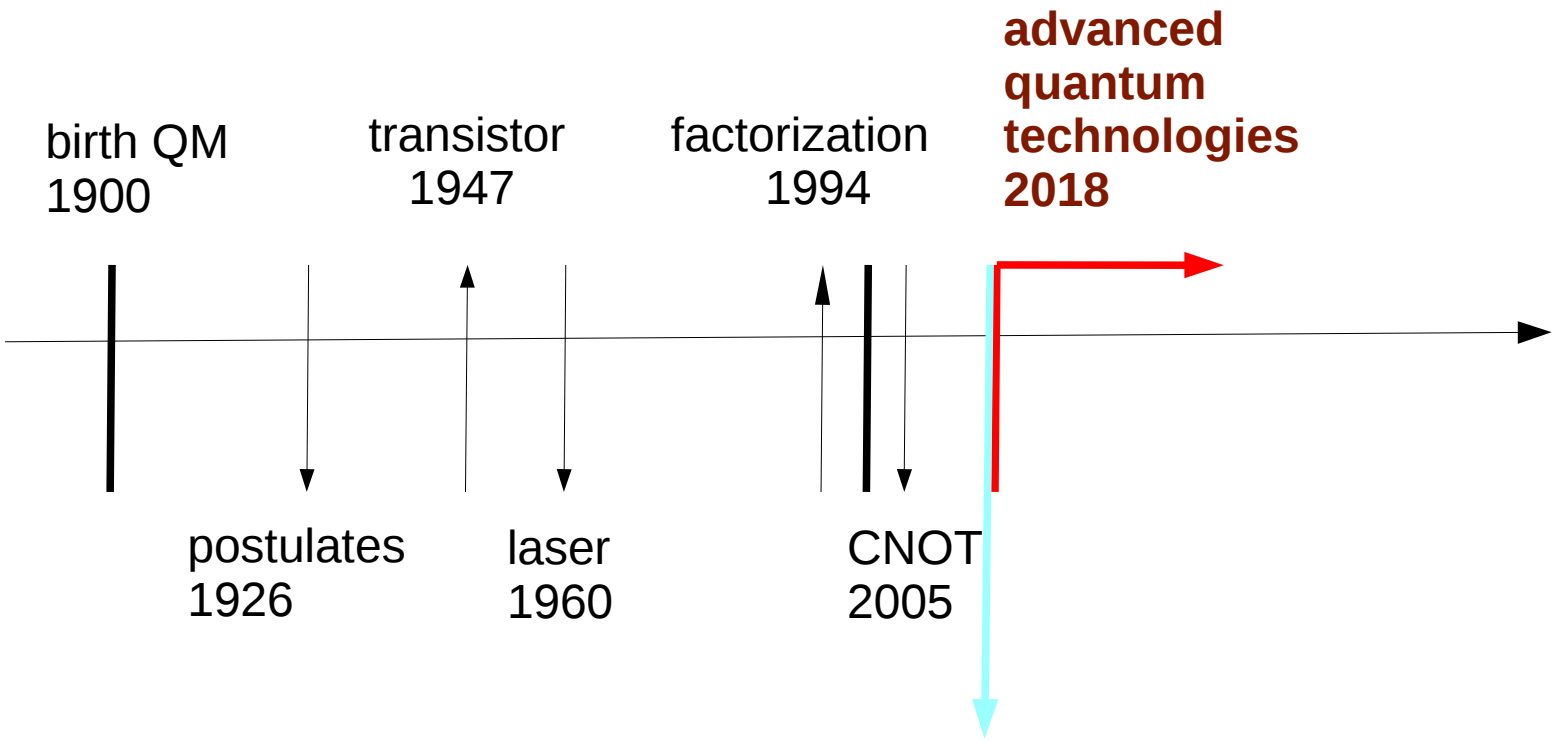
[1]Volkswagen Group of America, San Francisco, USA
[2]Volkswagen Data:Lab, Munich, Germany
[3]D-Wave Systems, Inc., Burnaby, Canada

Abstract

Quantum annealing algorithms belong to the class of meta-heuristic tools, applicable for solving binary optimization problems. Hardware implementations of quantum annealing, such as the quantum processing units (QPUs) produced by D-Wave Systems, have been subject to multiple analyses in research, with the aim of characterizing the technology's usefulness for optimization and sampling tasks. In this paper, we present a real-world application that uses quantum technologies. Specifically, we show how to map certain parts of a real-world traffic flow optimization problem to be suitable for quantum annealing. We show that time-critical optimization tasks, such as continuous redistribution of position data for cars in dense road networks, are suitable candidates for quantum computing. Due to the limited size and connectivity of current-generation D-Wave QPUs, we use a hybrid quantum and classical approach to solve the traffic flow problem.



Second Quantum Revolution

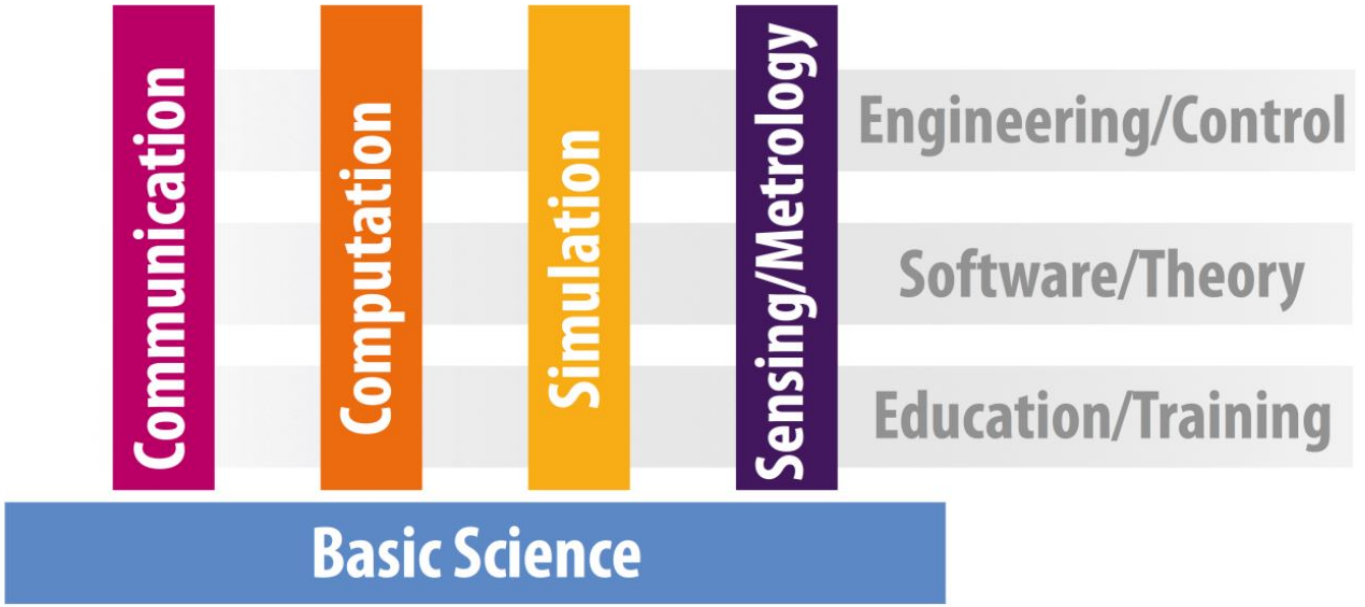


AI
Deep Machine Learning

Matter dominated

- Single atom
- Single photon
- Low temperatures
- ...

ET Flagship
Quantum Technologies



… back to physics

Computing
with
Quantum Mechanics

QM ➡ Information

Von Neumann & Copenhagen interpretation

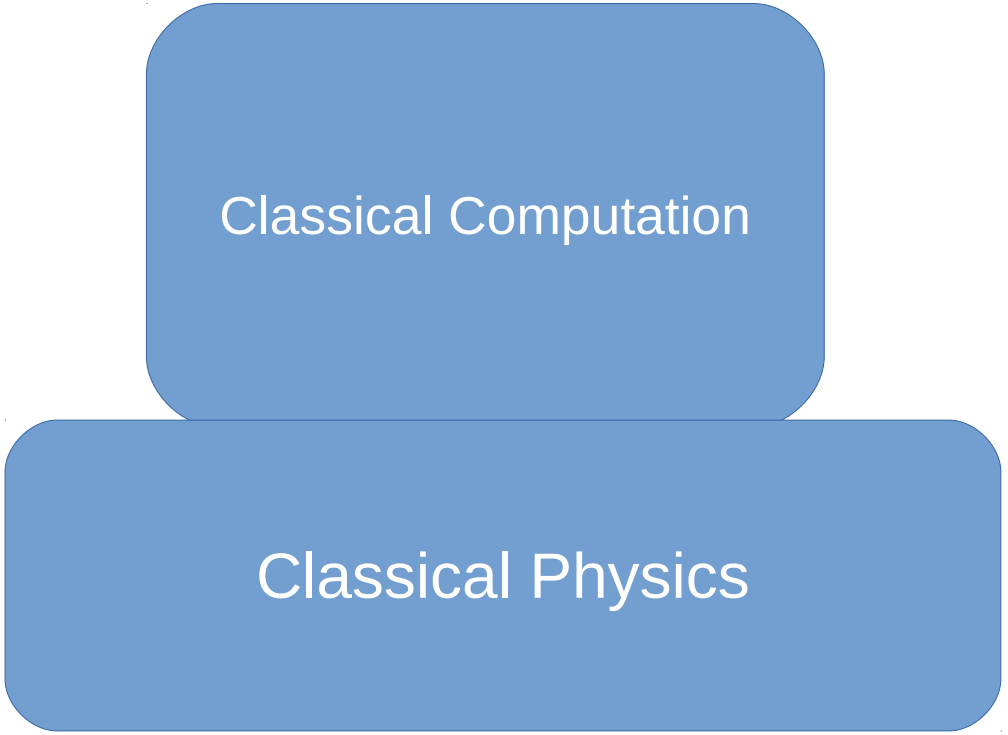
Postulate I
Ket keeps all available information on a system

Postulate II
Observables are related to operators acting on kets

Postulate III
Measurement collapses information
Born rule dictates this probabilistic collapse

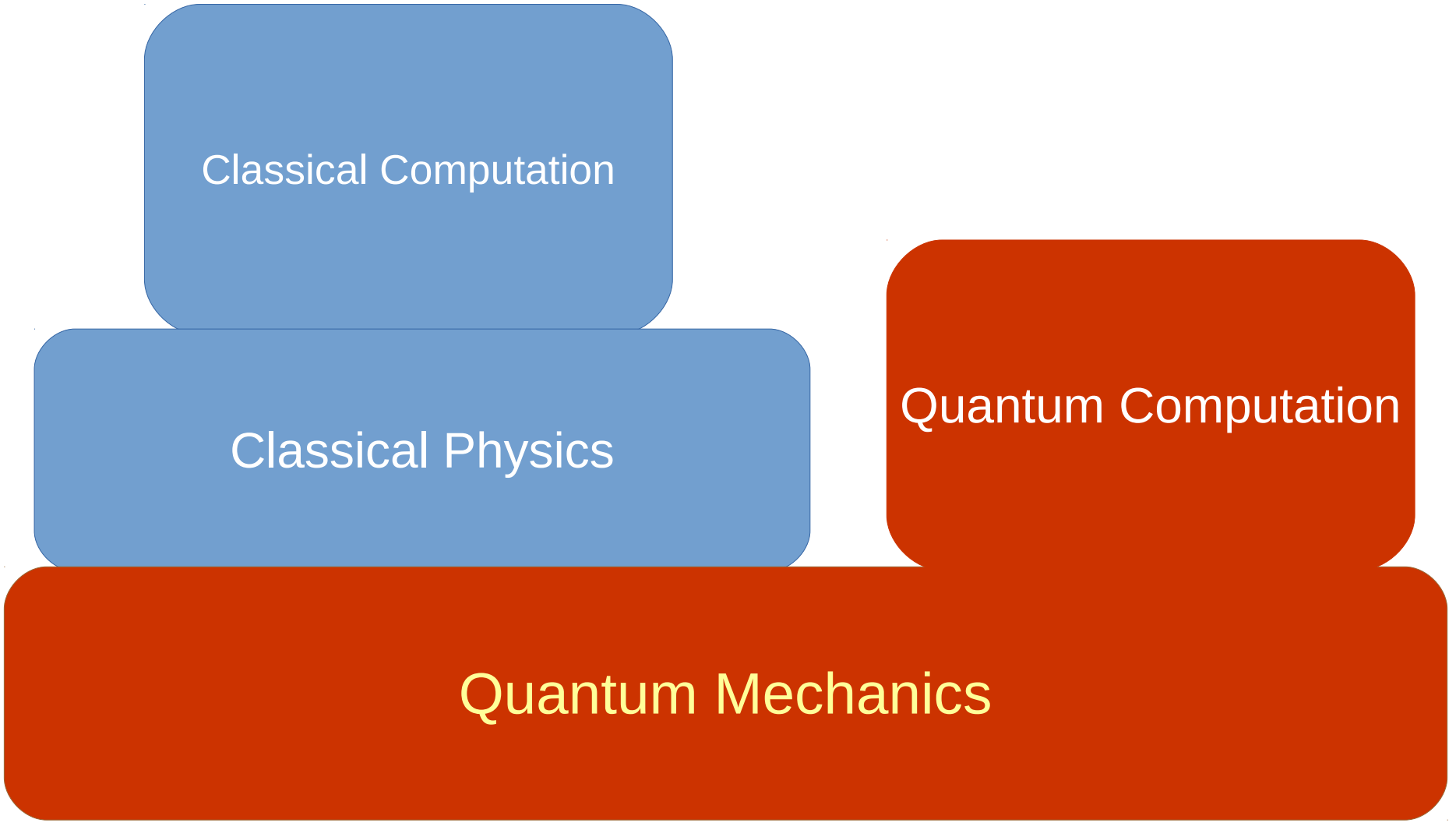
Postulate IV
Evolution is unitary and deterministic, keeps probabilities

Information ➡ QM



Church, Post, Turing,...: Computing = Physics

Information ➡ QM



Feynman: Computing with QM

Physics

Logical bit

$|0\rangle$

$|1\rangle$

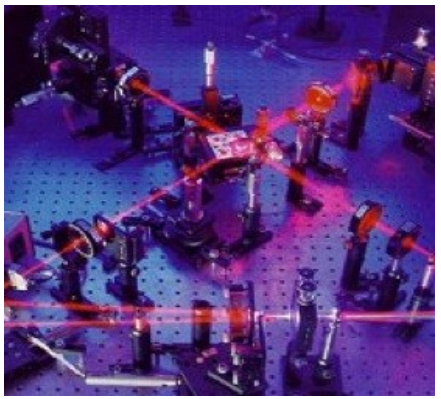
Superposition

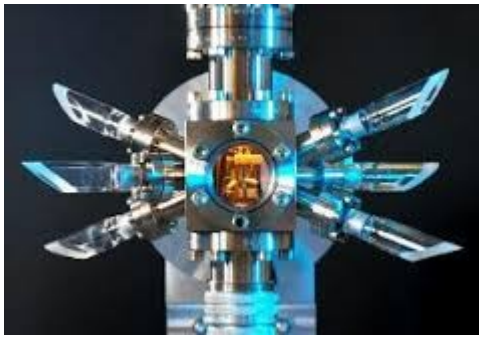
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

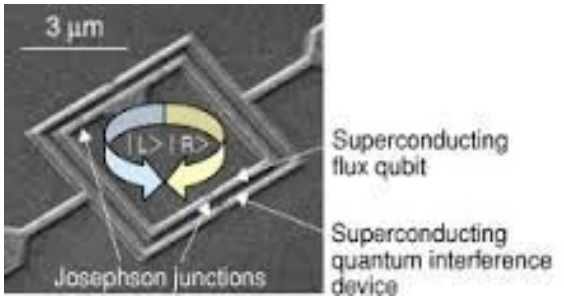
Physical implementations

Quantum Cryptography

Quantum Computation







Photons:
H-V polarization
Time bins

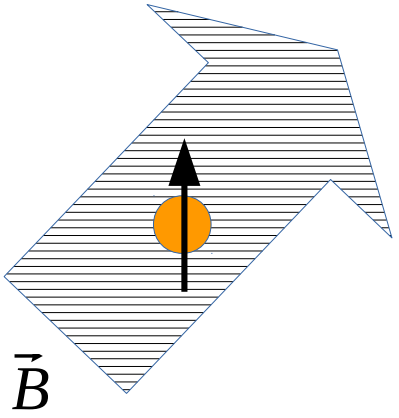
Trapped ions:
ground-excited energy

Superconducting curents:
Left-right rotation

QUBIT

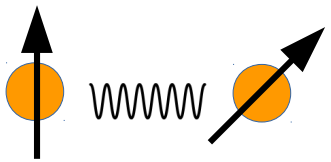
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Unitary Evolution = Quantum Gates



$$U_H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$U_H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$



$$U_{CNOT}|00\rangle = |00\rangle \qquad U_{CNOT}|10\rangle = |11\rangle$$

$$U_{CNOT}|01\rangle = |01\rangle \qquad U_{CNOT}|11\rangle = |10\rangle$$

New Logical Gates

Interference

Quantum advantatge

Massive superpositions for computation!

$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} \left| i_1, i_2, \ldots, i_n \right\rangle$$

2^n superpositions on ***n*** qubits

1 register of 50 qubits contains more information than any classical computer

Massive parallel computation!

$$U|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} U \left| i_1, i_2, \ldots, i_n \right\rangle$$

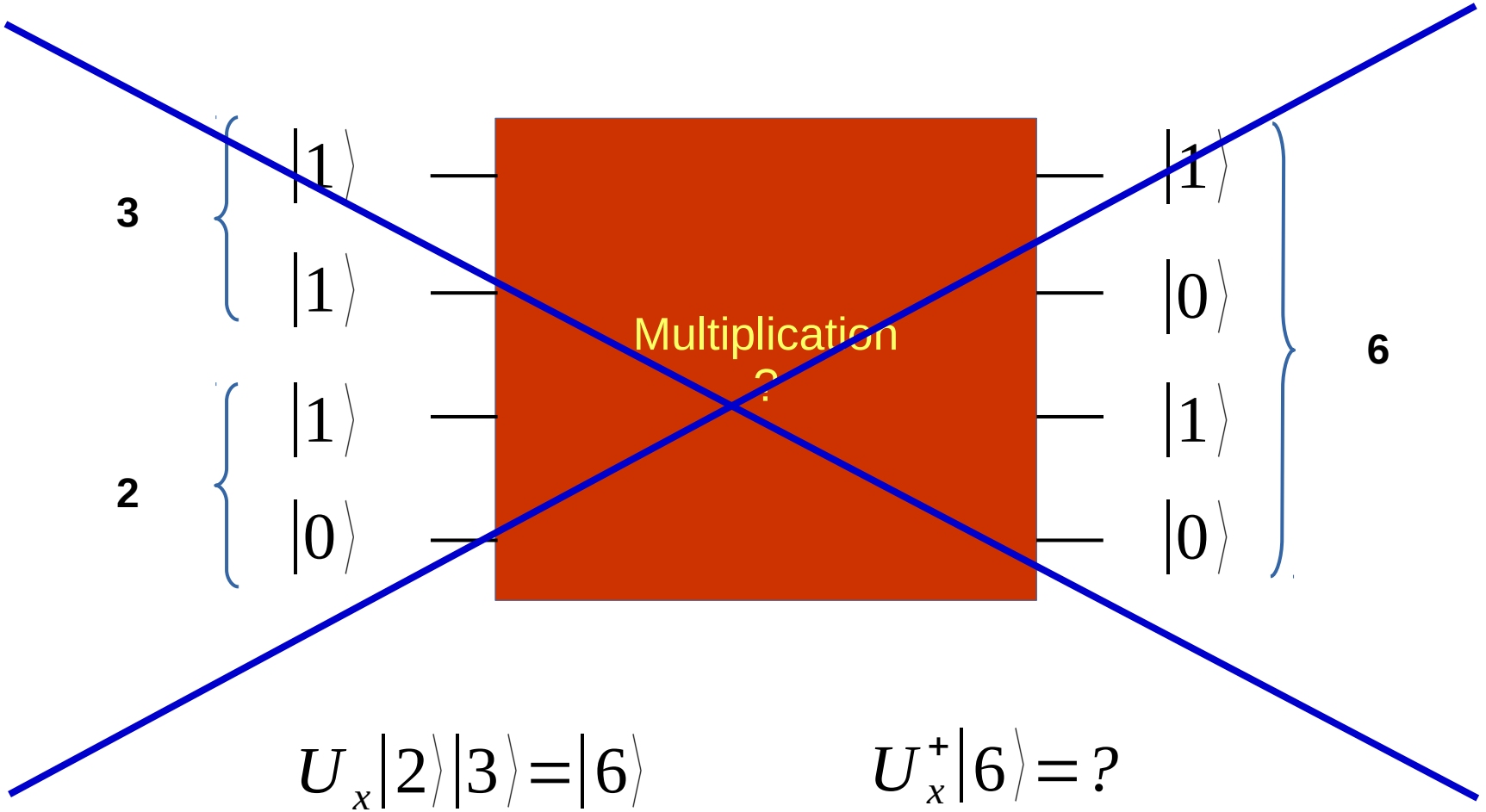
BUT

Quantum Mechanics follows its on laws

Multiplication

$$U_x|2\rangle|3\rangle=|6\rangle$$

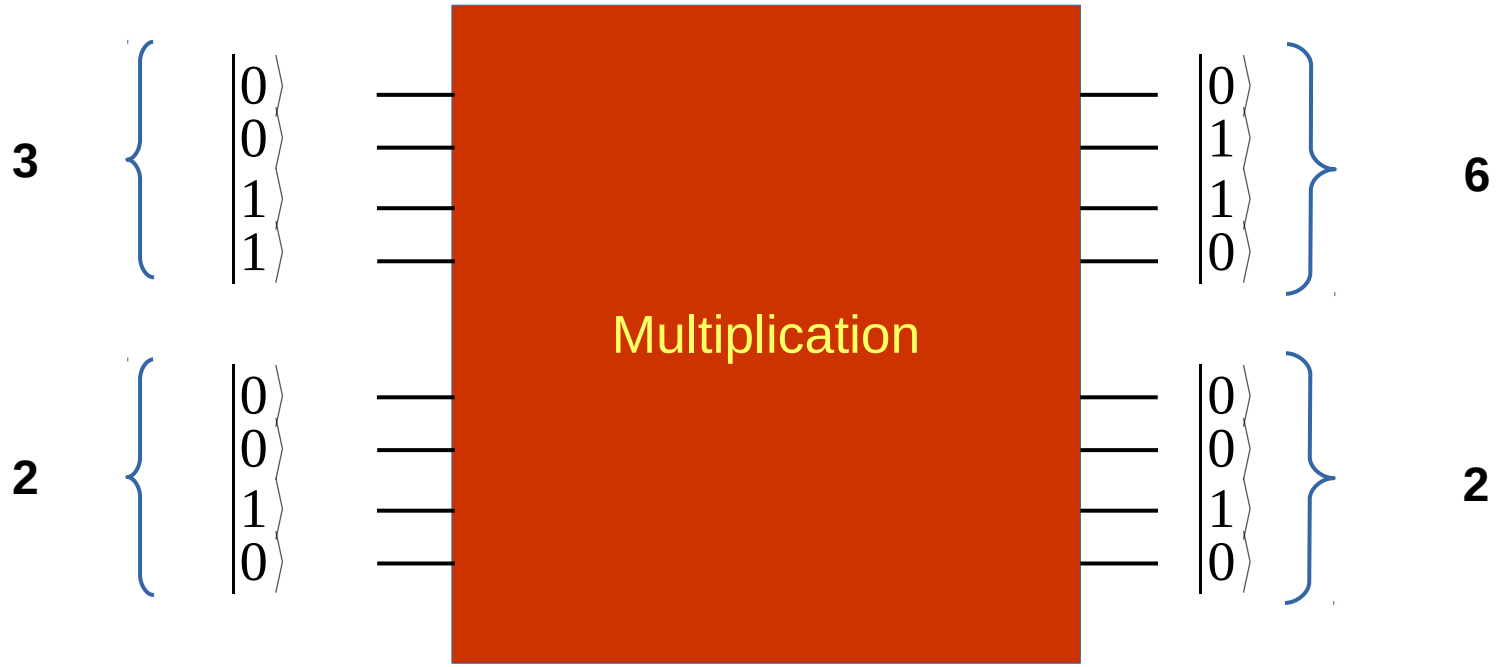
Multiplication



$$U_x|2\rangle|3\rangle = |6\rangle \qquad U_x^+|6\rangle = ?$$

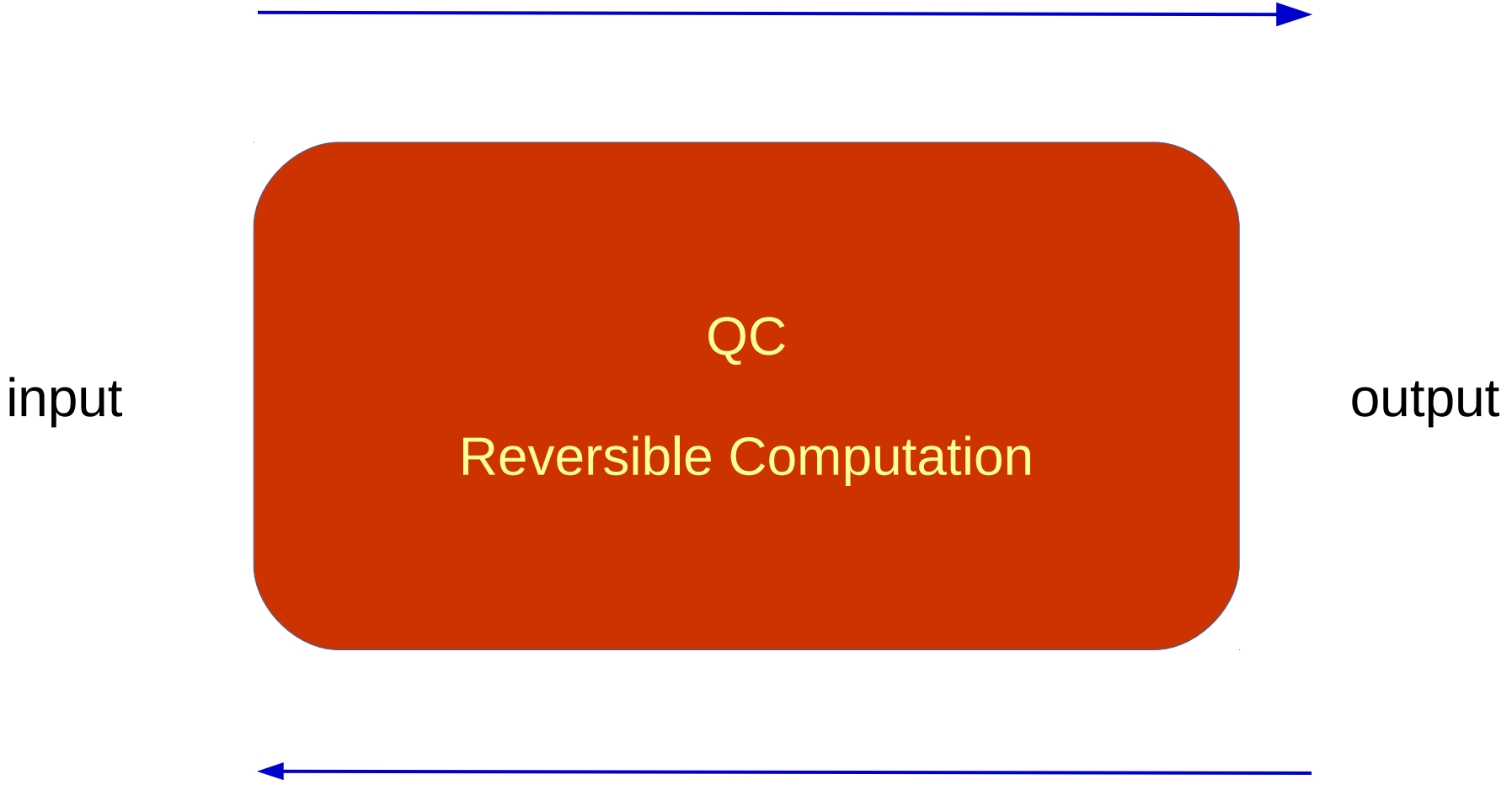
NOT UNITARY

Unitarity = Reversible Computation

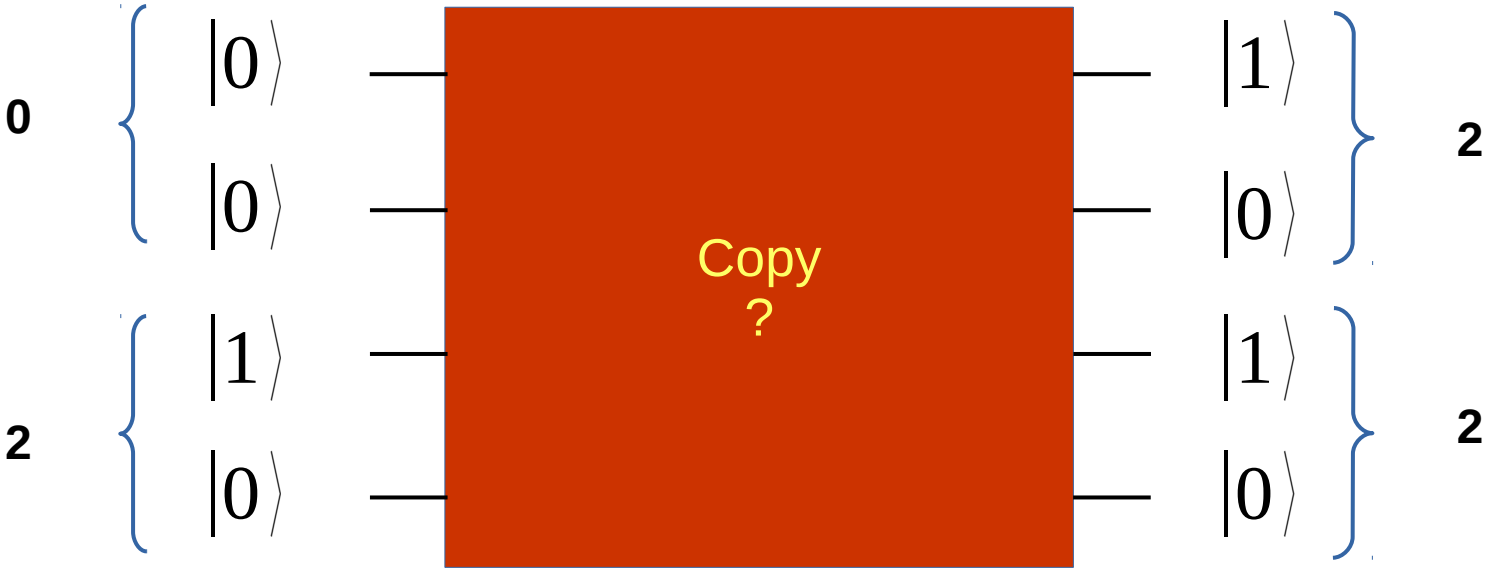


$$U_x|2\rangle|3\rangle = |2\rangle|6\rangle$$

$$U_x|x\rangle|y\rangle = |x\rangle|f(x,y)\rangle$$

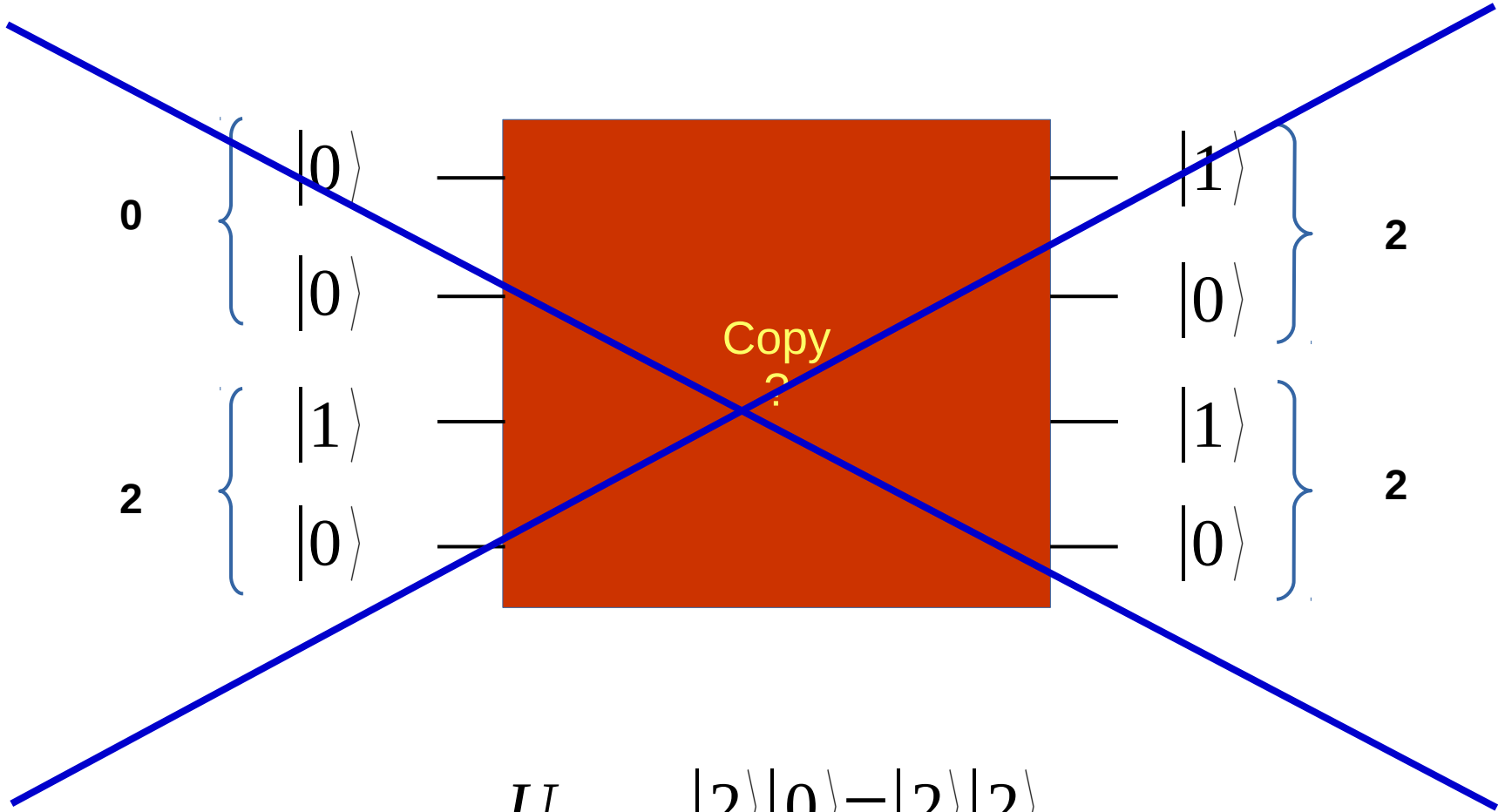

input
QC
Reversible Computation
output

Copy



$$U_{cloning}|2\rangle|0\rangle=|2\rangle|2\rangle$$

Copy



$$U_{cloning}|2\rangle|0\rangle=|2\rangle|2\rangle$$

NO CLONING

No cloning theorem

$$U_{cloning}|0\rangle|a\rangle=|0\rangle|0\rangle$$
$$U_{cloning}|1\rangle|a\rangle=|1\rangle|1\rangle$$

$$U_{cloning}(c_0|0\rangle+c_1|1\rangle)|a\rangle=c_0|0\rangle|0\rangle+c_1|1\rangle|1\rangle$$

$$\neq(c_0|0\rangle+c_1|1\rangle)(c_0|0\rangle+c_1|1\rangle)$$

No cloning underlies

- no inference for the exact result of a measurement
- no violation of causality
- no breaking quantum cryptography,….

Measurement

Inherent quantum randomness

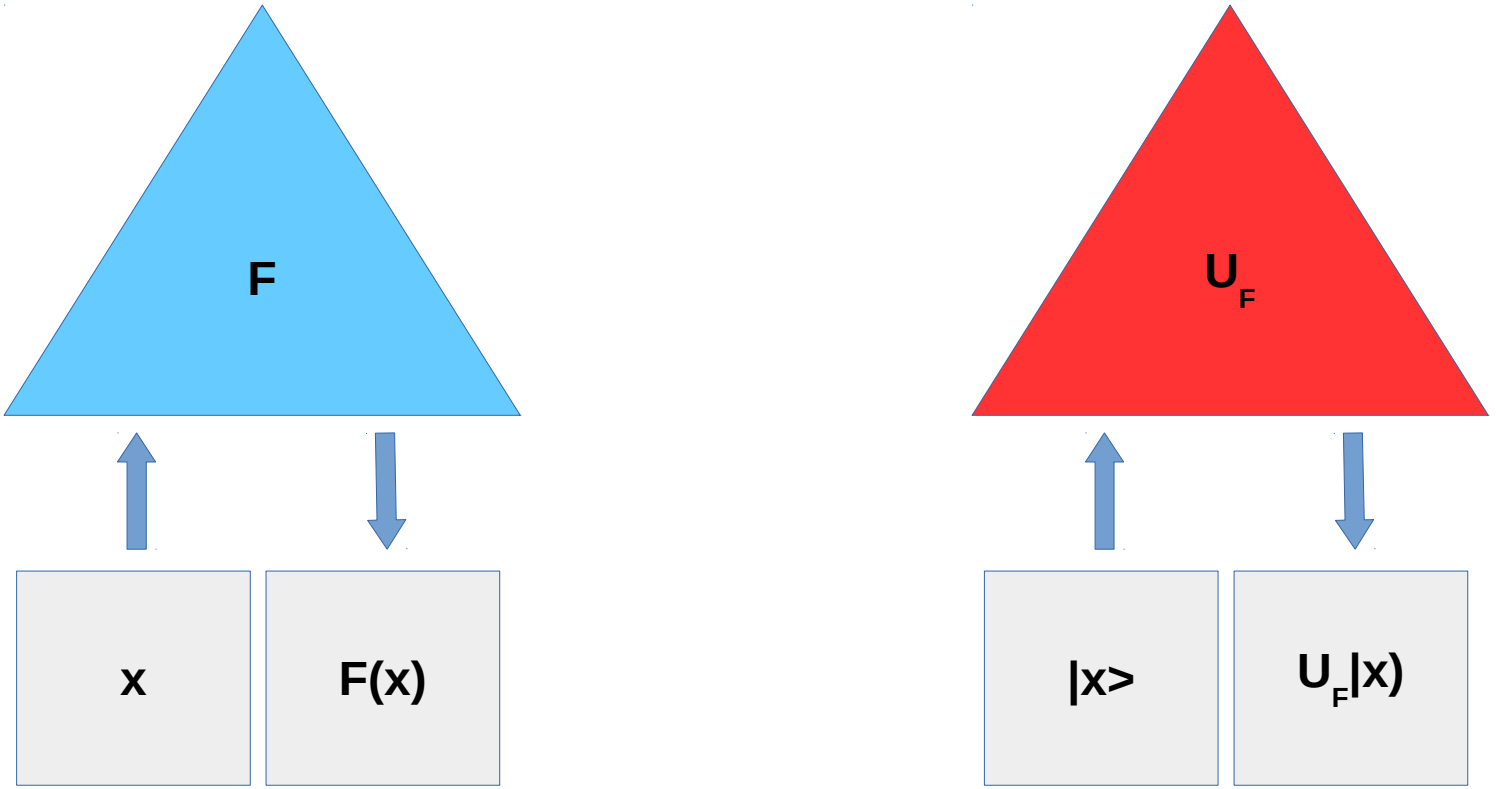
$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} \left| i_1, i_2, \ldots, i_n \right\rangle$$

$$P\left(i_1, i_2, \ldots, i_n\right) = \left| c_{i_1, i_2, \ldots, i_n} \right|^2$$

The magic of

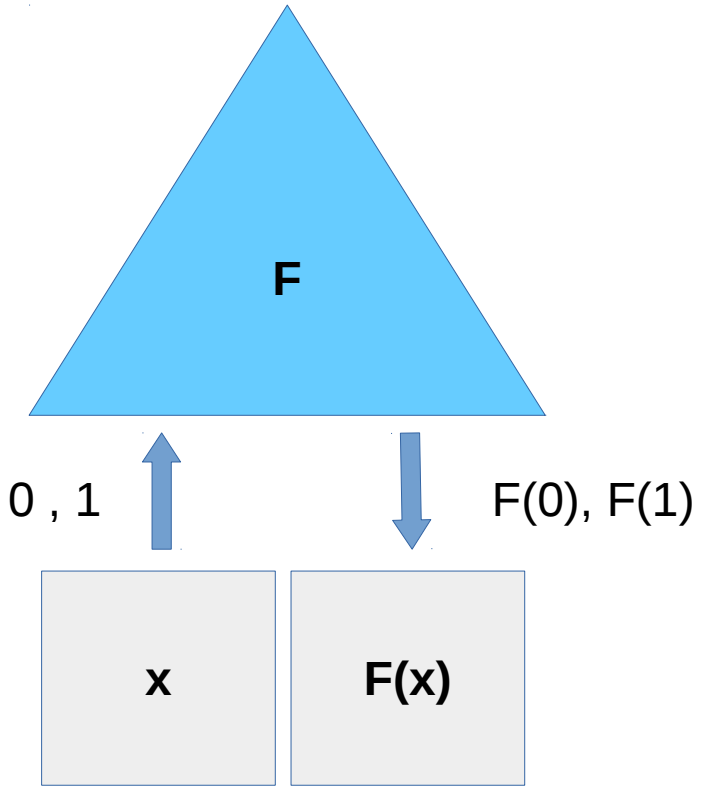
Quantum Algorithms

Queries to an **oracle**



Can QM reduce the number of calls to an oracle?

Queries to an **oracle**



Simplest example: is F constant?

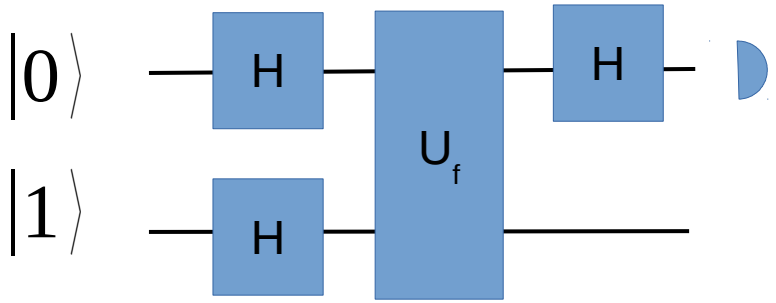
$$F:\{0,1\}\rightarrow\{0,1\}$$

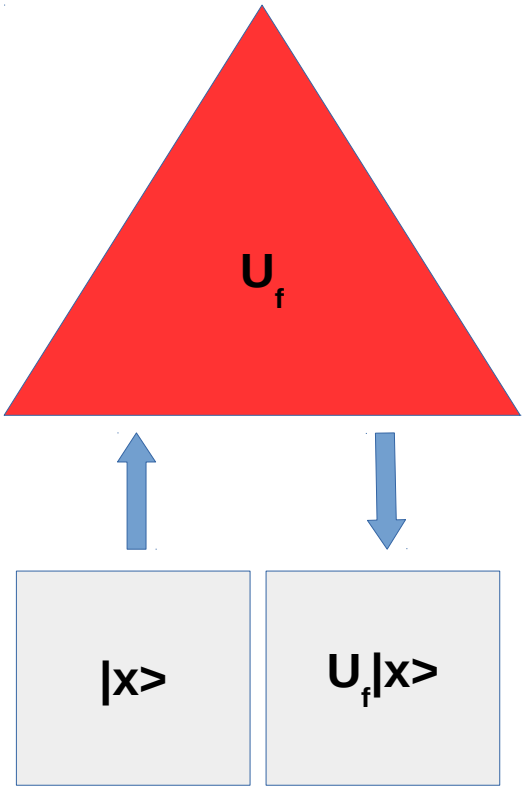
$$F(0)=F(1)\,?$$

$$F(0)\neq F(1)\,?$$

Classically, we need two calls to know if F is balanced

Queries to an **oracle**





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

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

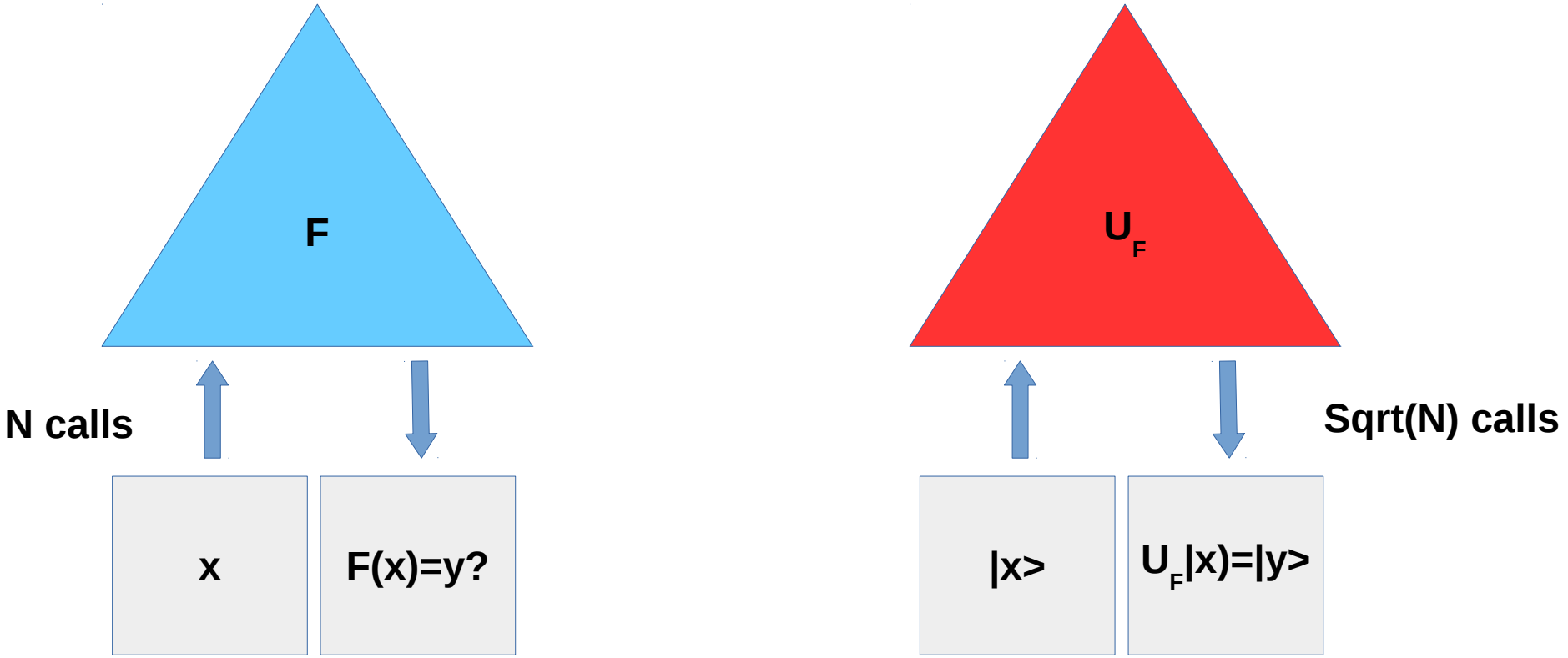
$$|0\rangle(|0+f(0)\rangle-|1+f(0)\rangle)+|1\rangle(|0+f(1)\rangle-|1+f(1)\rangle)$$

$$(|0\rangle+(-1)^{f(0)+f(1)}|1\rangle)(|0\rangle-|1\rangle)$$

$$(1+(-1)^{f(0)+f(1)})|0\rangle+(1-(-1)^{f(0)+f(1)})|1\rangle$$

QM needs a single call to the oracle!!

Queries to an oracle: **search an unstructured database**



Grover's algorithm

Solve a hash, bitcoin!

Factorization

$$N = p\,q$$

Choose a and find r such that $a^r = 1 \bmod(N)$

i) r is not even
ii) r is even and $a^{r/2} = -1 \bmod(N)$
iii) r is even and $a^{r/2} \neq -1 \bmod(N)$

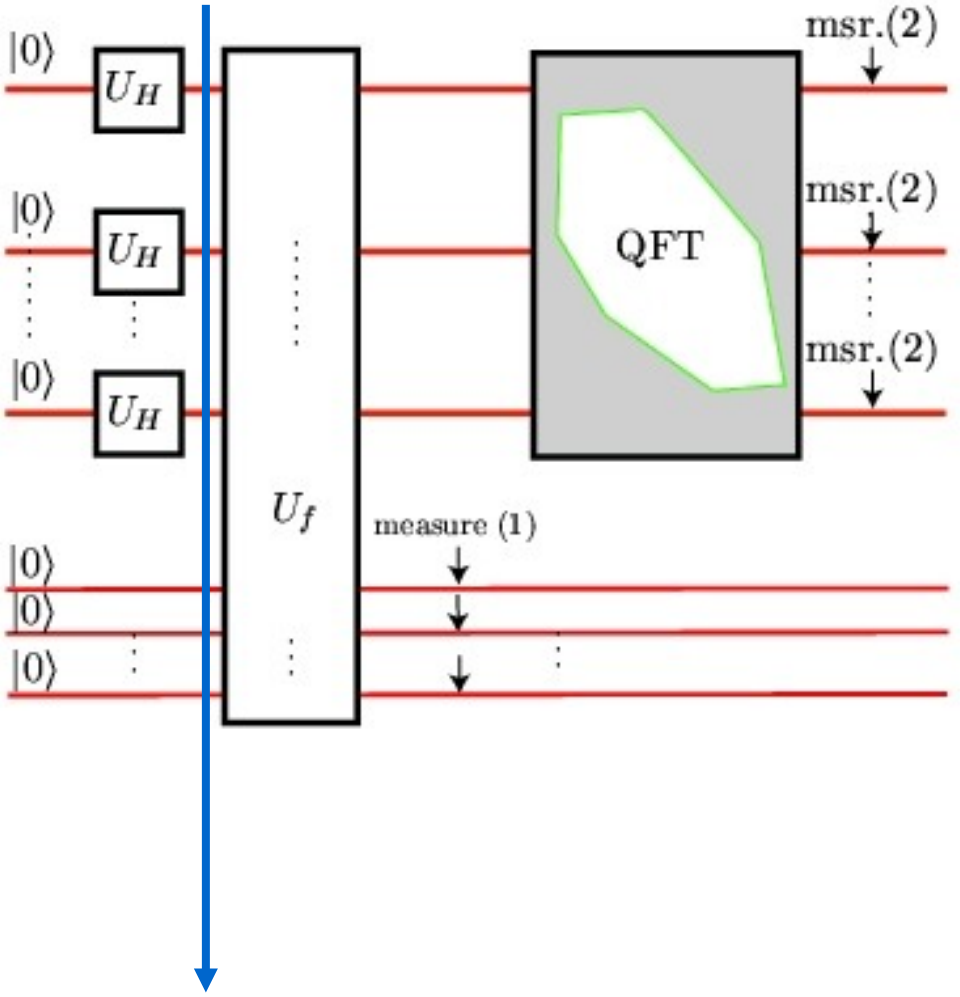
If iii) $p = \gcd(N, a^{r/2} + 1)$ $q = \gcd(N, a^{r/2} - 1)$

Factoring = Finding a hidden period

Shor's algorithm

1. Initialize register and ancillae

$$|\psi\rangle = |00\ldots0\rangle_{target}\,|00\ldots0\rangle_{ancillae}$$

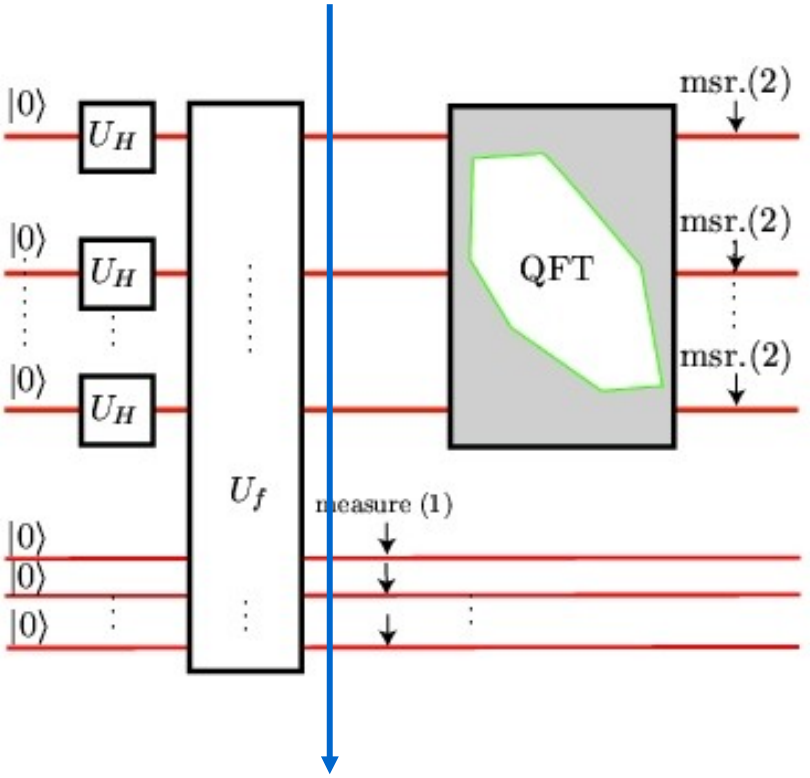


2. Create superposition of all solutions

$$U_H^{(1)} \otimes U_H^{(2)} \ldots \otimes U_H^{(n)} |\psi\rangle = \sum_{x=0,\ldots,2^n-1} |x\rangle_{target}\,|00\ldots0\rangle_{ancillae}$$

3. Apply modular exponentiation

$$\sum_{x=0,\ldots,2^n-1} \left|x\right\rangle_{target} \left|a^x \bmod (N)\right\rangle_{ancillae}$$

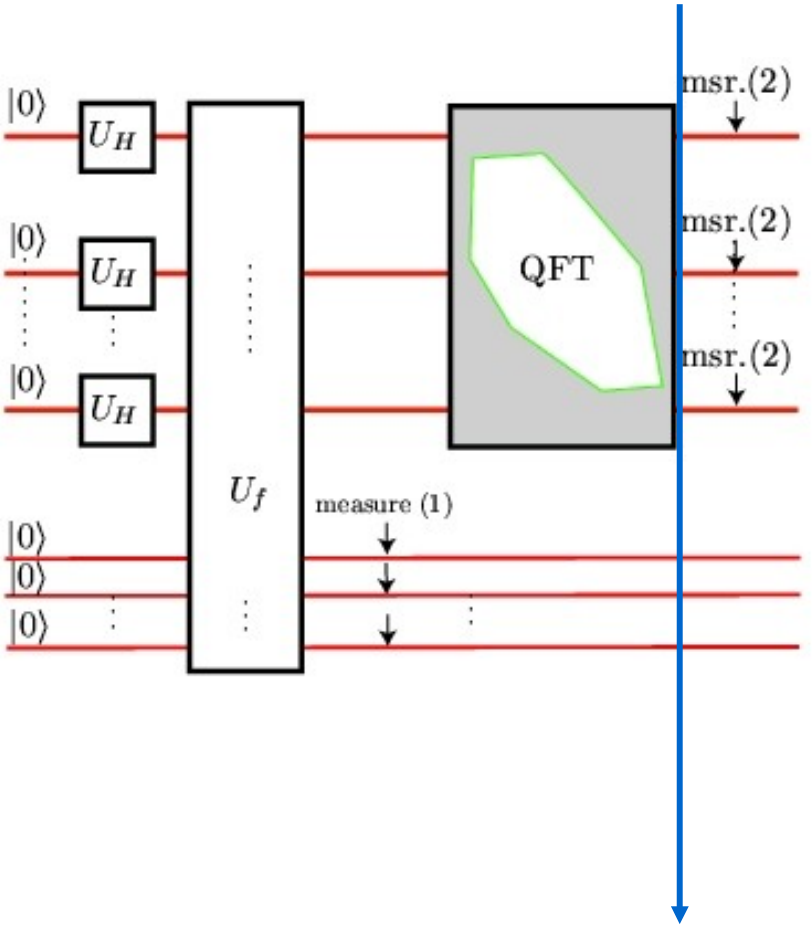


4. Measure ancillae

$$\sum_k \left|d_b + k\,r\right\rangle_{target} \left|b\right\rangle_{ancillae}$$

A period has been created!!!

5. Perform Quantum Fourier Transform



QFT is efficient!!!!

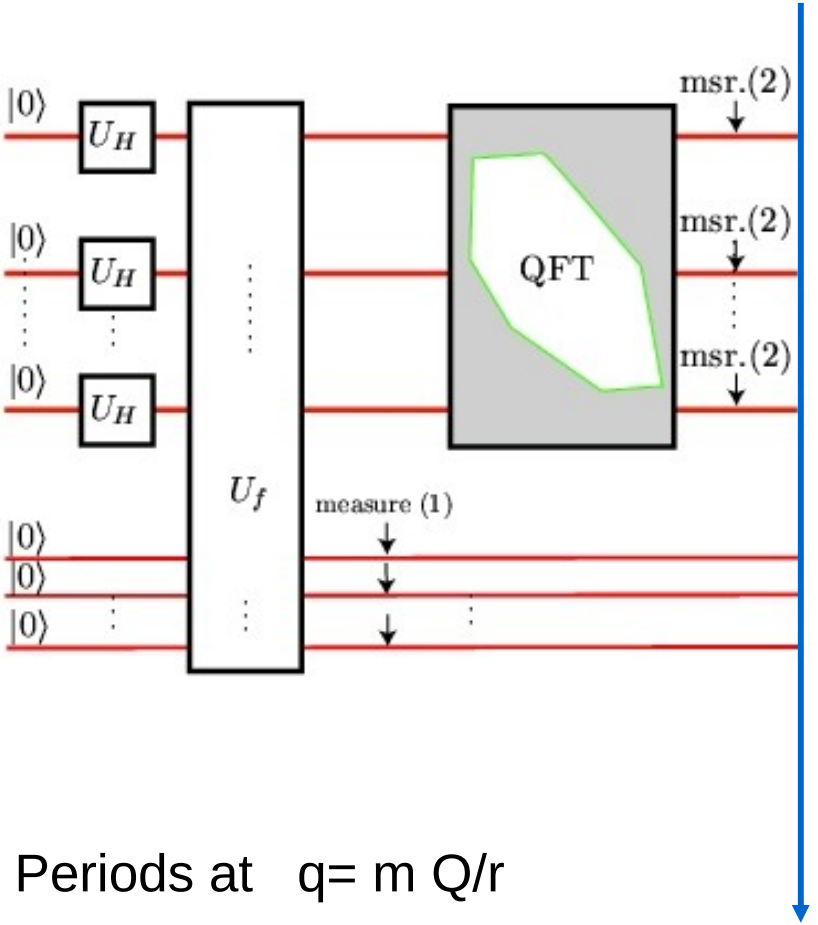
Polynomial in QM

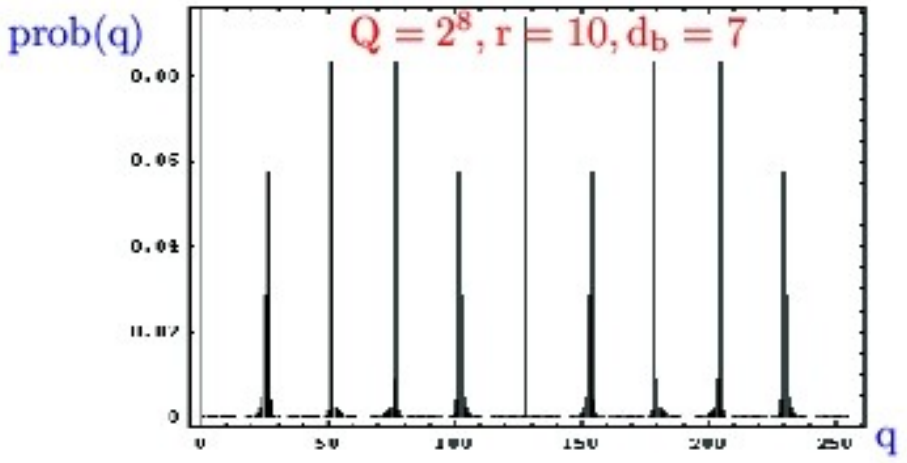
Exponential in Classical

$$\sum_q \sum_k e^{i q 2\pi (d_b + k r)} |q\rangle_{target} |b\rangle_{ancillae}$$

6. Measure the target

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





Periods at q= m Q/r

read r

Factorization (Quantum Fourier Transform)

Classical Computer

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

Quantum Computer

$$n^3 (\log n)(\log(\log n))$$

Quantum exponential speedup

Sooner than later

A Quantum Computer will factor larger numbers efficiently!!!

RSA/DSA/ECC classical cryptography will be broken

Are we ready for that?

Connectivity

NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn't yet know what to do about that problem.

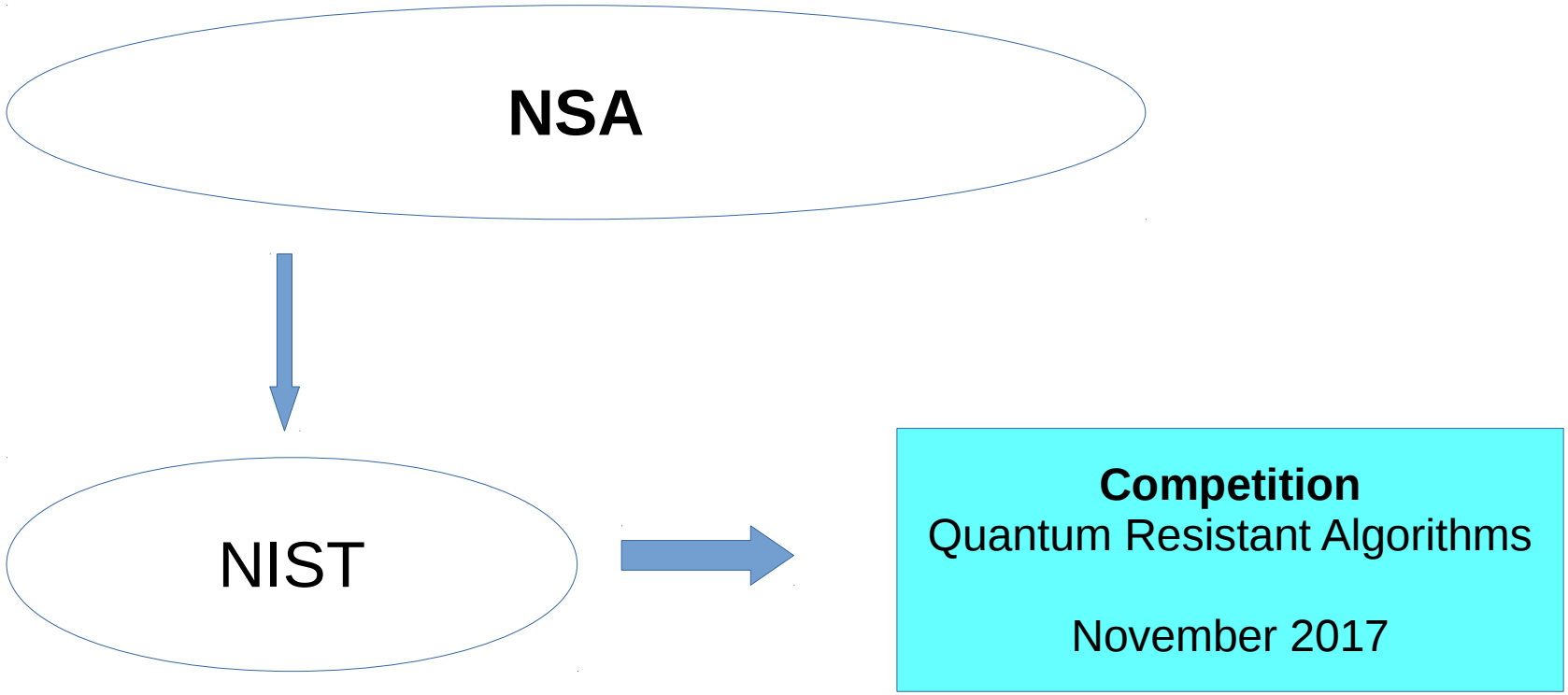
The NSA remarked that "The AES-256 and SHA-384 algorithms are symmetric, and believed to be safe from attack by a large quantum computer."

According the NSA, the following isn't safe to use:

- ECDH and ECDSA with NIST P-256
- SHA-256
- AES-128
- RSA with 2048-bit keys
- Diffie-Hellman with 2048-bit keys

What provoked this switch was the ever-growing threat of quantum computers breaking encryption.

"... quantum computers will use "qubits" that behave in surprising ways, efficiently performing selected mathematical algorithms exponentially faster than a classical computer." The NSA went on to say "A sufficiently large quantum computer, if built, would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures."

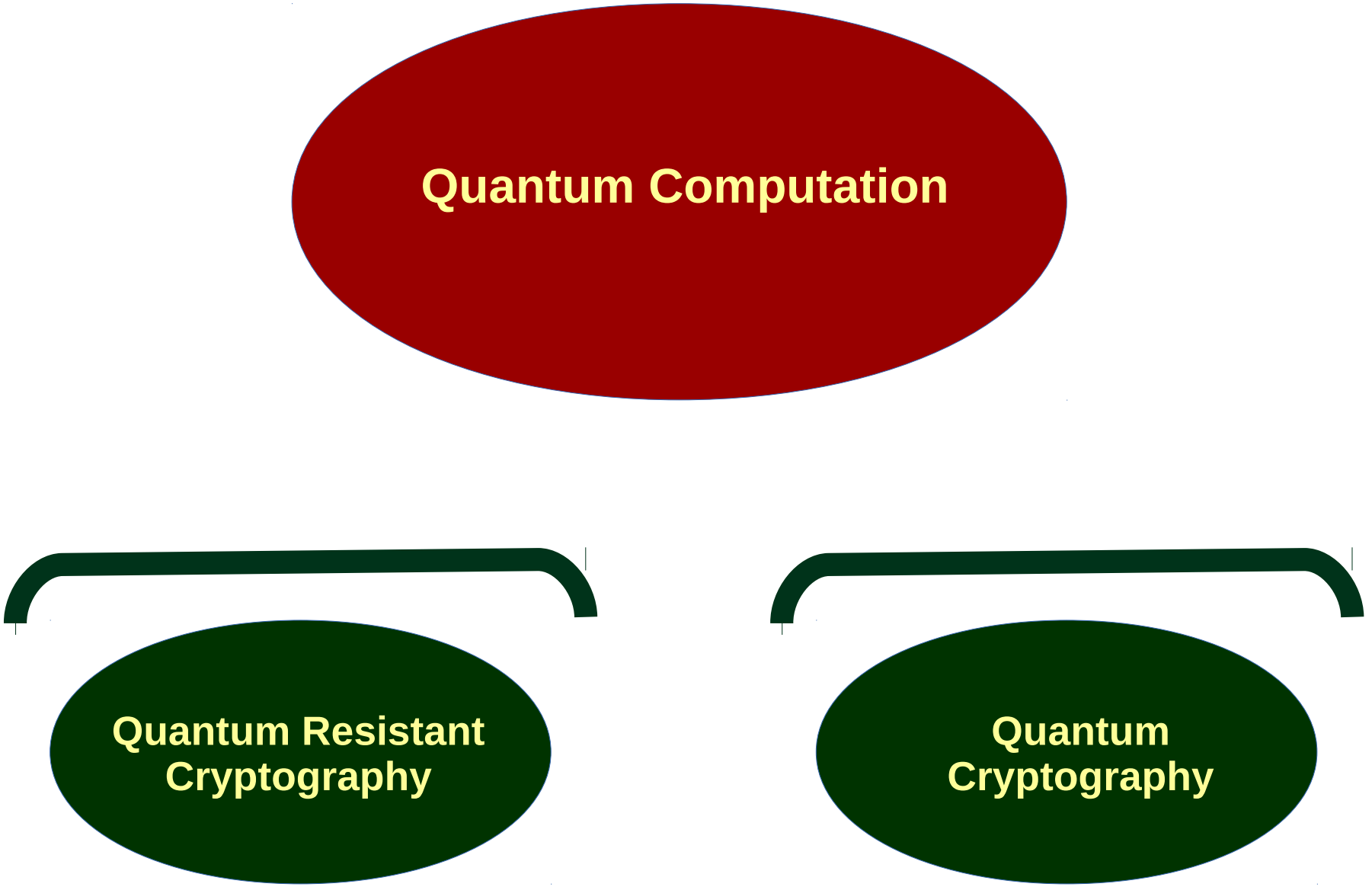

NSA
NIST
Competition
Quantum Resistant Algorithms
November 2017

Quantum Resistant (Post-Quantum) Algorithms

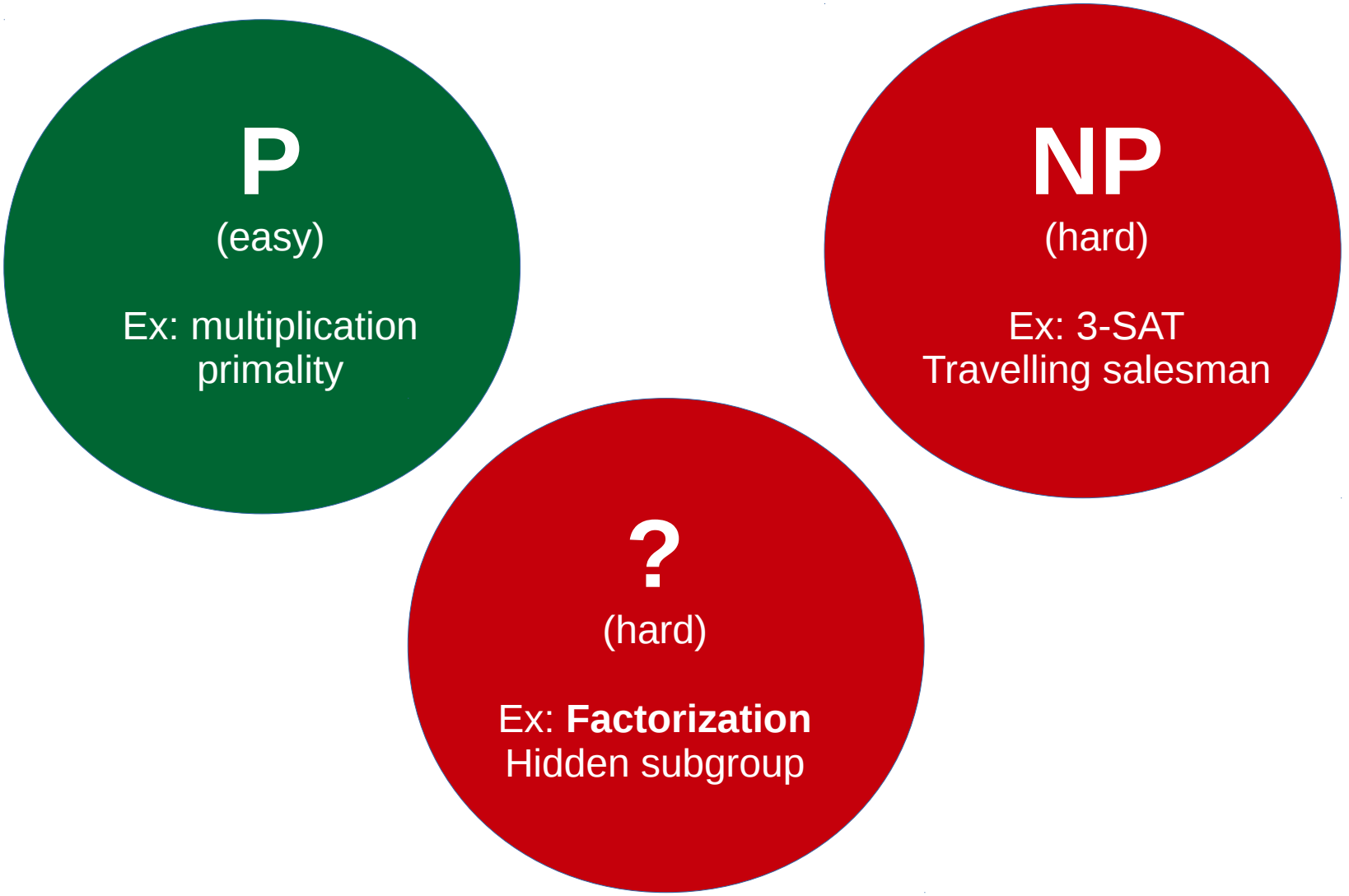
- Lattice-based
  Ring-LWE (Ring Learn with Errors)
- Code-based
  McEliece
- Hash-based
  Merkel signature
- ….

Somewhat based on NP-hard problems
All add structure to NP-hard to make easy-encryption&hard-decryption
They may all be broken by a quantum computer, but there is no evidence

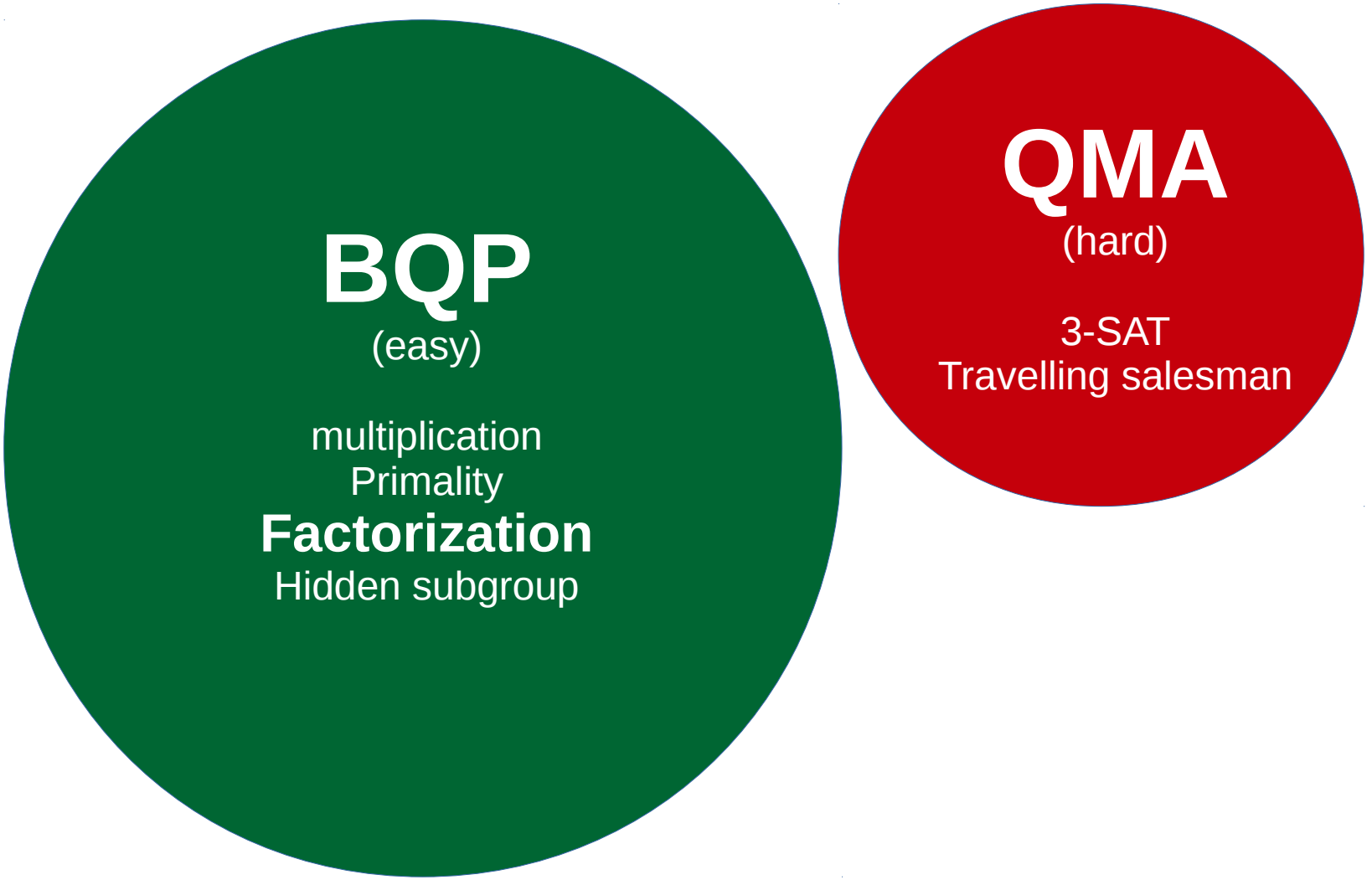
No provable security

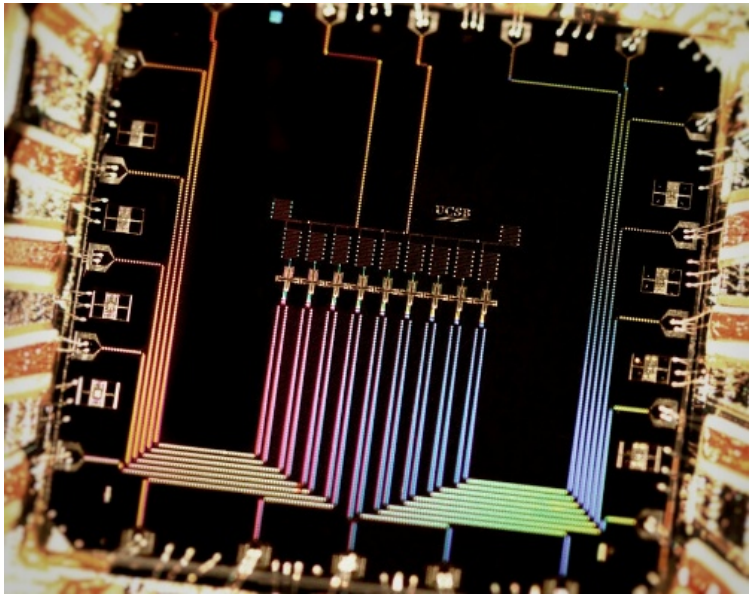

Quantum Computation
Quantum Resistant Cryptography
Quantum Cryptography

Which problems can be solved with a Classical Computer?

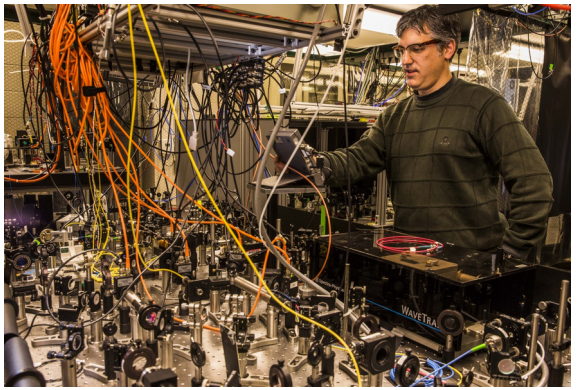


Which problems can be solved with a Quantum Computer?

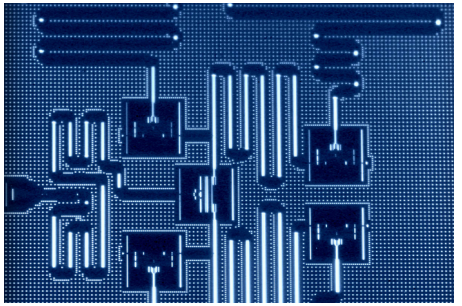




Martinis (Google)



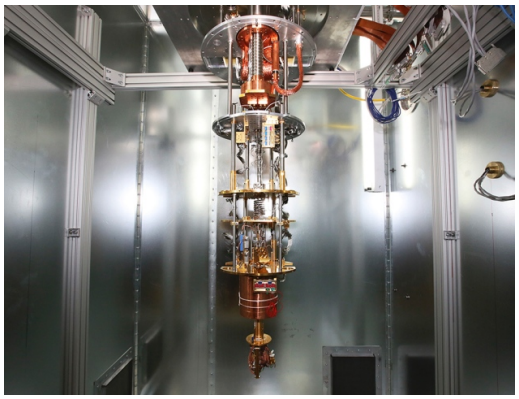
ionQ



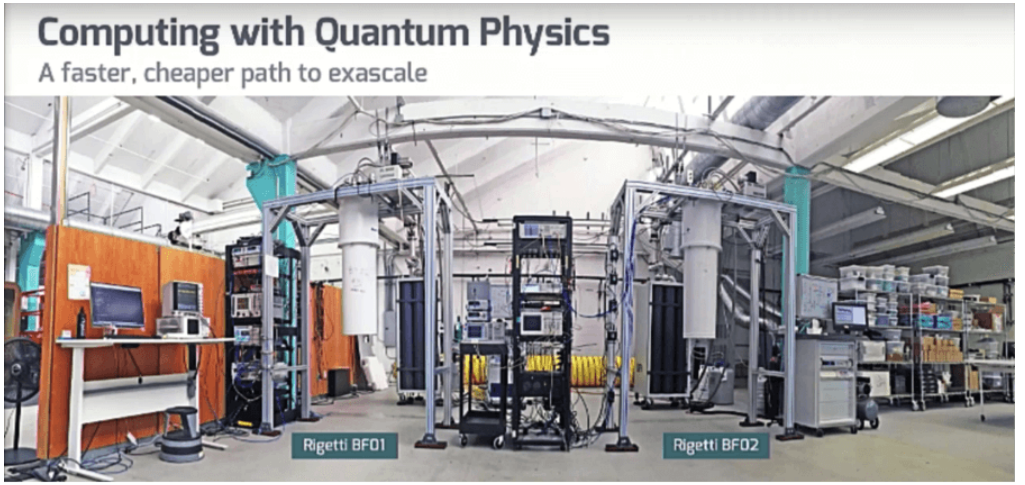
IBM cloud computer

STATION Q

Microsoft



DWAVE2



Rigetti

+LABS all over the world

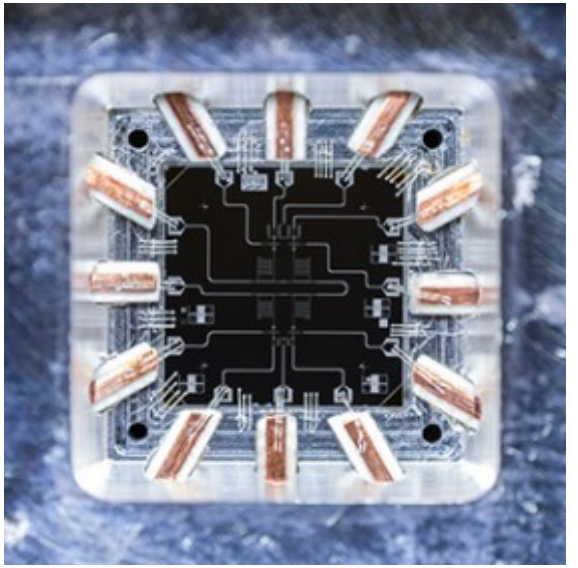
Recent Progress

Google 9, 22 qubit experiment

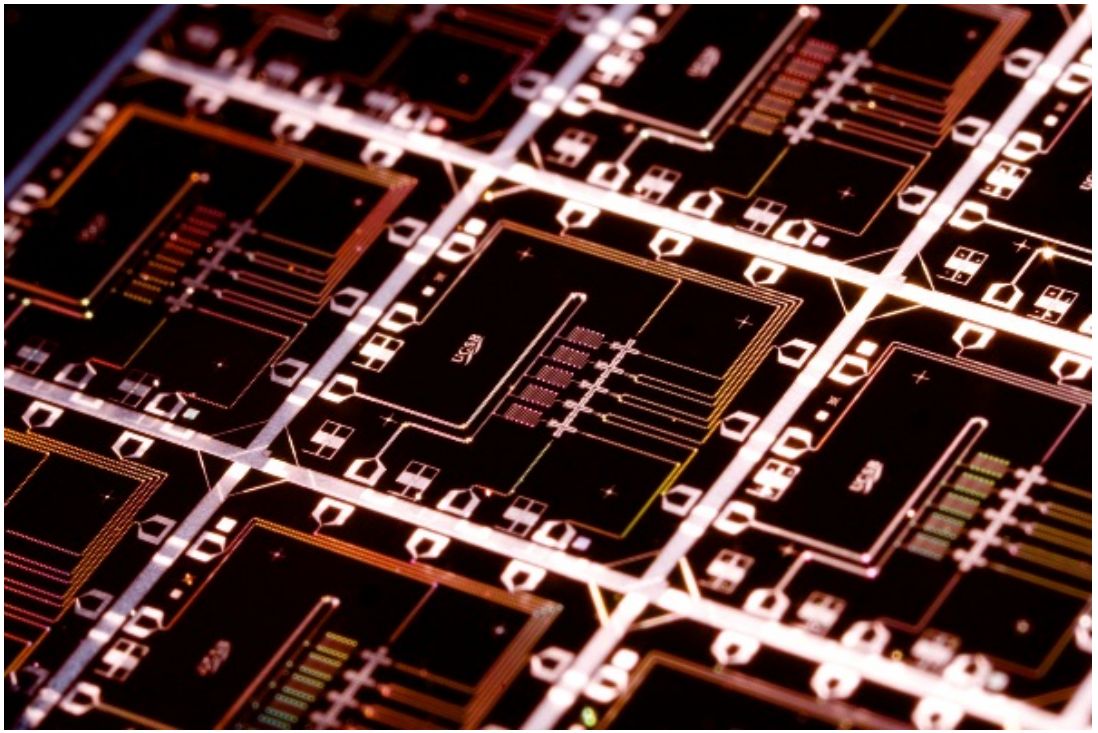
Rigetti 19 qubit

IBM commercial 20 qubit

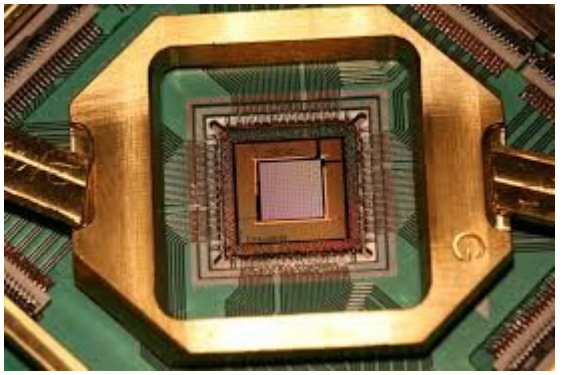
Microsoft ?? qubit



Google: Quantum Supremacy
50 qubits
Bosonic sampling

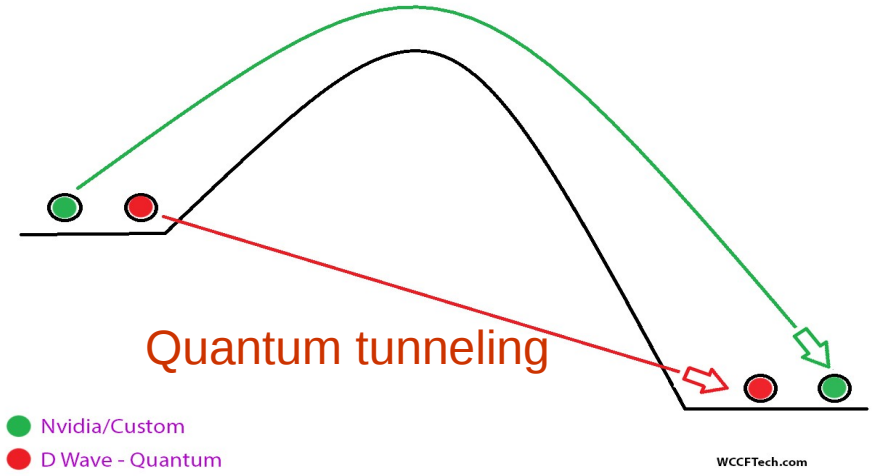


Annealing



DWAVE-2 2048 qubits
Optimization problems, no error correction

Tunnel across the barrier!!



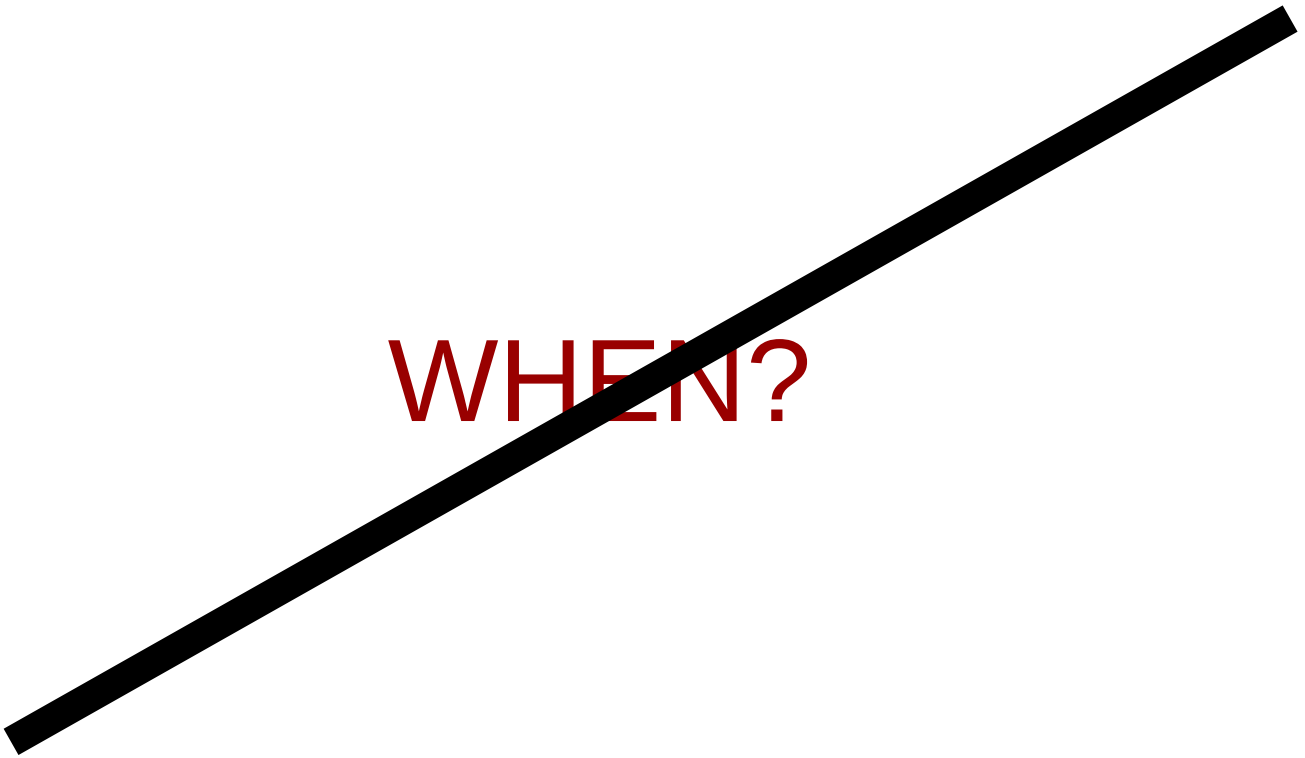
Quantum Computing for

- **Breaking classical crypto**
- **Interplay with AI**
- **Optimization problems**
  - Traffic flow
  - **Quantum chemistry**
  - Scheduling
  - ...

BIG QUESTION

WHEN?

Quantum Supremacy: Martinis 2018


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?

“Who?” includes us?

QUANTIC

@ BSC/UB

Home | About | Research | Team | Publications | Collaborators | Offers | Funding | Contact

QuanTic@BSC-UB

A first qubit in the South of Europe is here!!

Quantum Hub

Quantum Experimental Lab: quantum annealer
Quantum Software Services

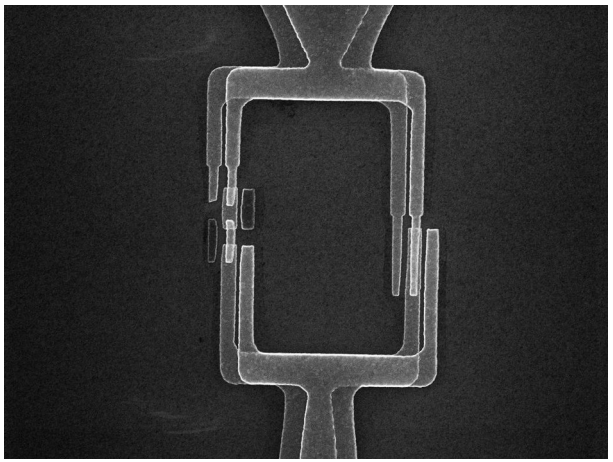
(Qilimanjaro cryptocurrency QBIT)

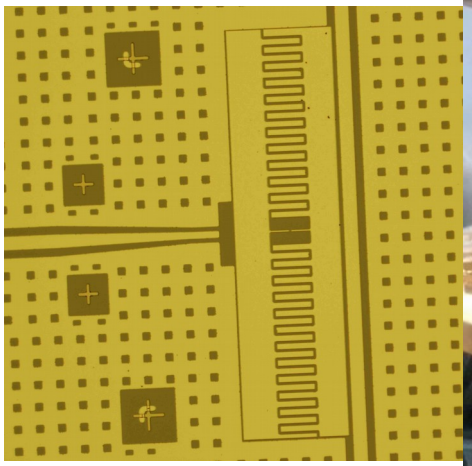
Experimental Lab

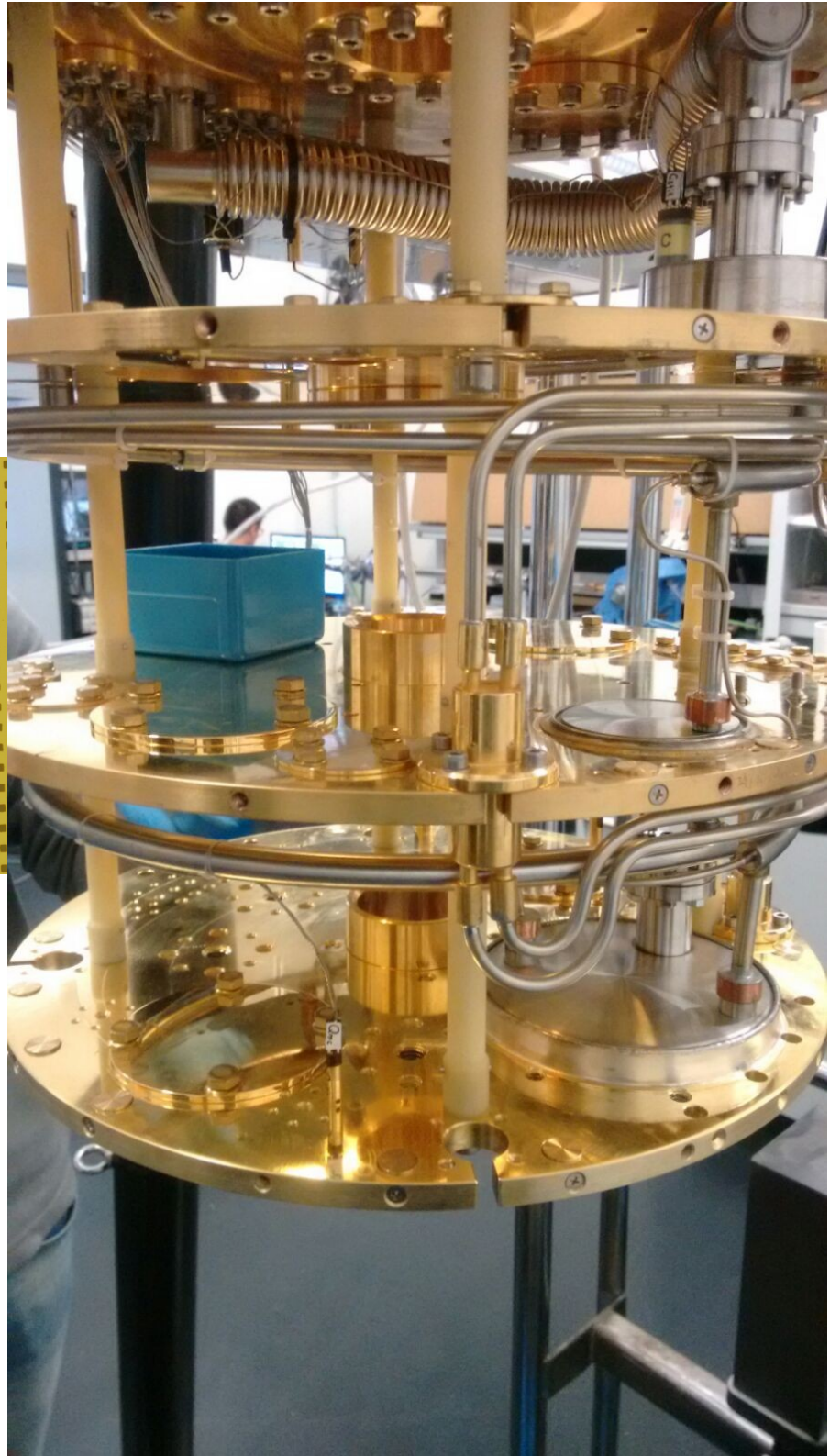
Quantum annealer based on fluxons

Pol Forn-Díaz

Christopher Warren







13 Partners

Glasgow, Karlsruhe, Grenoble, Munich, ETH, CSIC, EHU,UB
Metempsy, Keysight,
Repsol, Volkswagen, Google, D-Wave

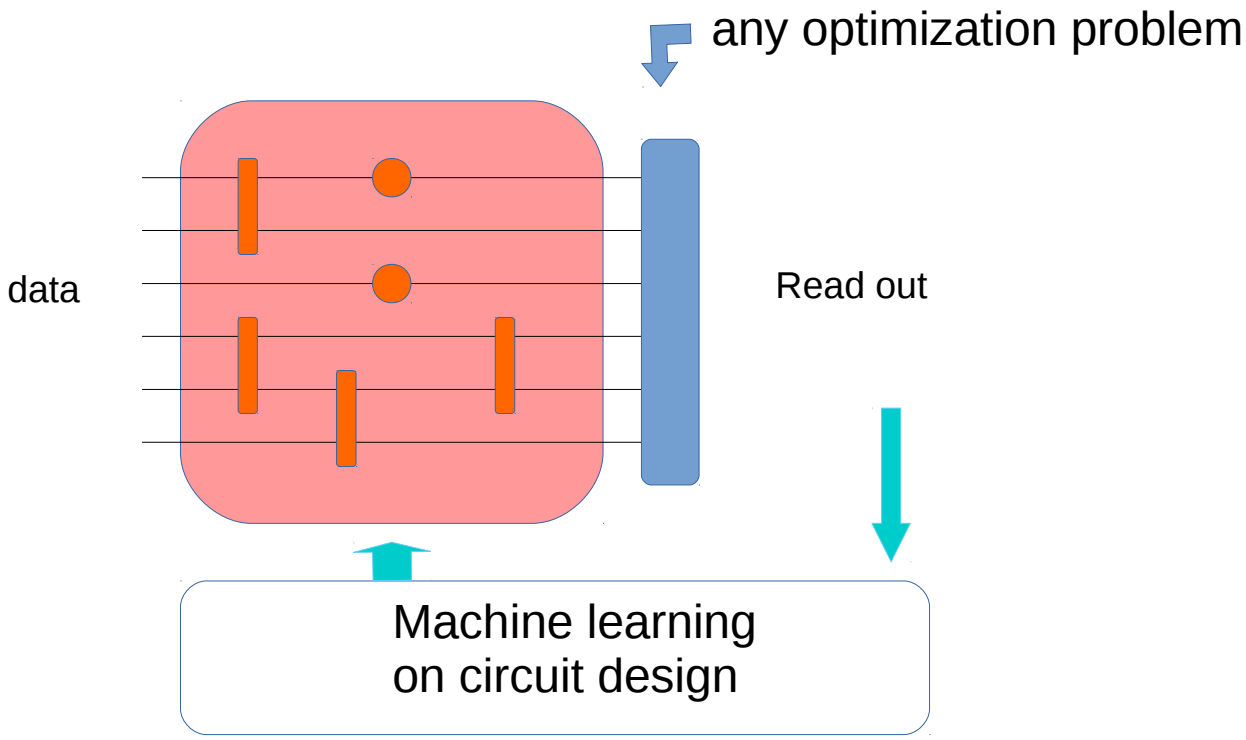
No need for error correction

10 qubits in 3 y

100 qubits in 6 y

Sofware Lab: Adiabatically Assisted Variational Quantum Eigensolvers

Artur García-Sáez
Alba Cervera-Lierta



Collaborations
IBM (BSC HUB)
Repsol
Internship program

CONCLUSION

Quantum computation
- Quantum Engineering

Quantum advantatge
- Speed, Size, Energy

New research strategies
- Partnerships with corporations
- New figures of merit (publications??)

Quantum Race
- Quantum supremacy
- Factorization
- (post)Quantum cryptography
- Quantum sensors

q-THANKS !!!!

QUANTUM CRYPTOGRAPHY

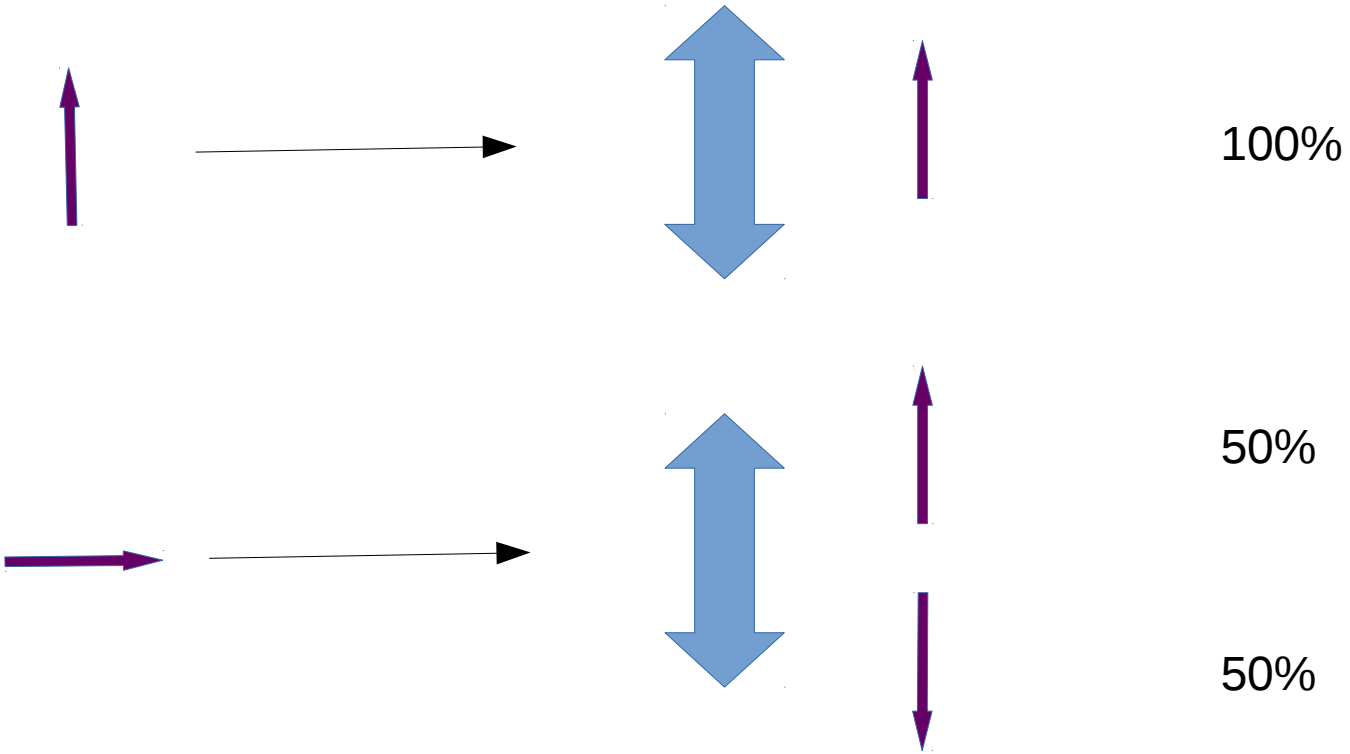
Key idea

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

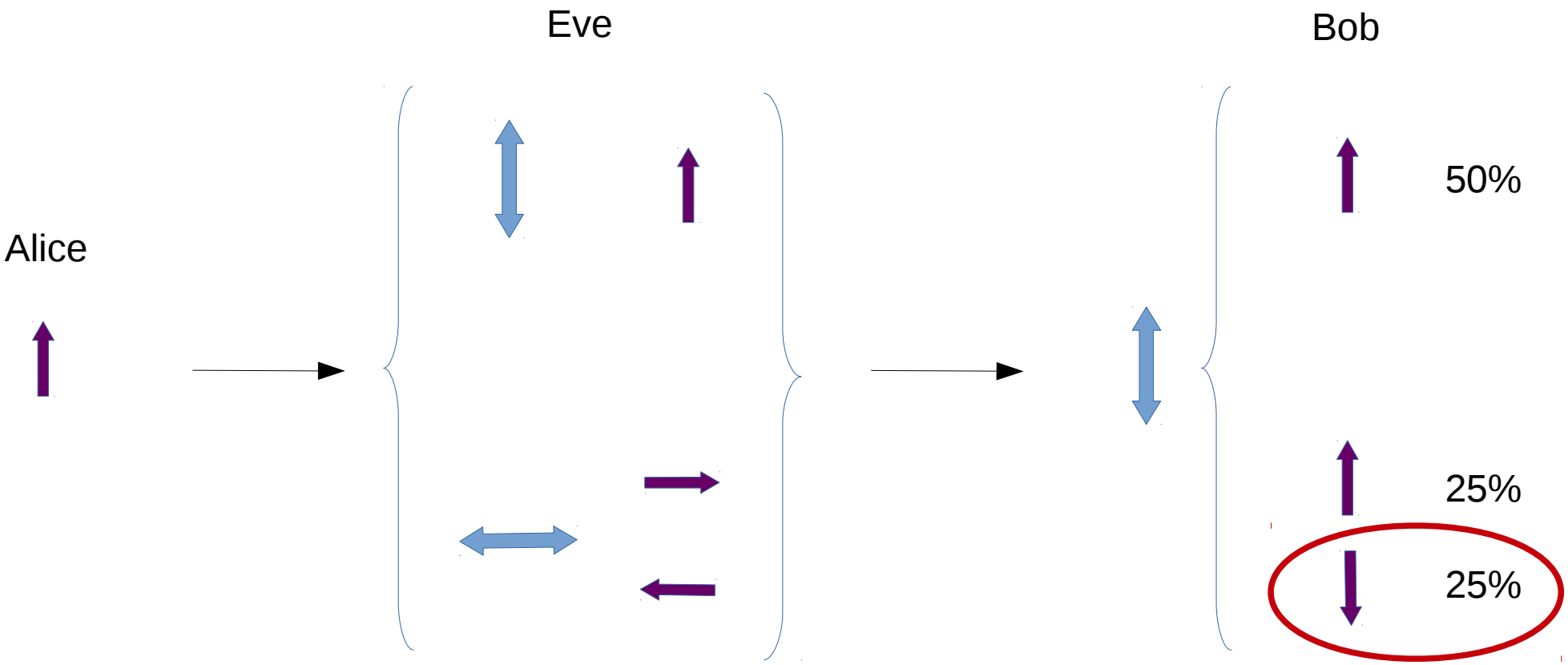
The process of observing a state **modifies** it in an uncontrolable way

The presence of Eve can be uncovered!

BB84

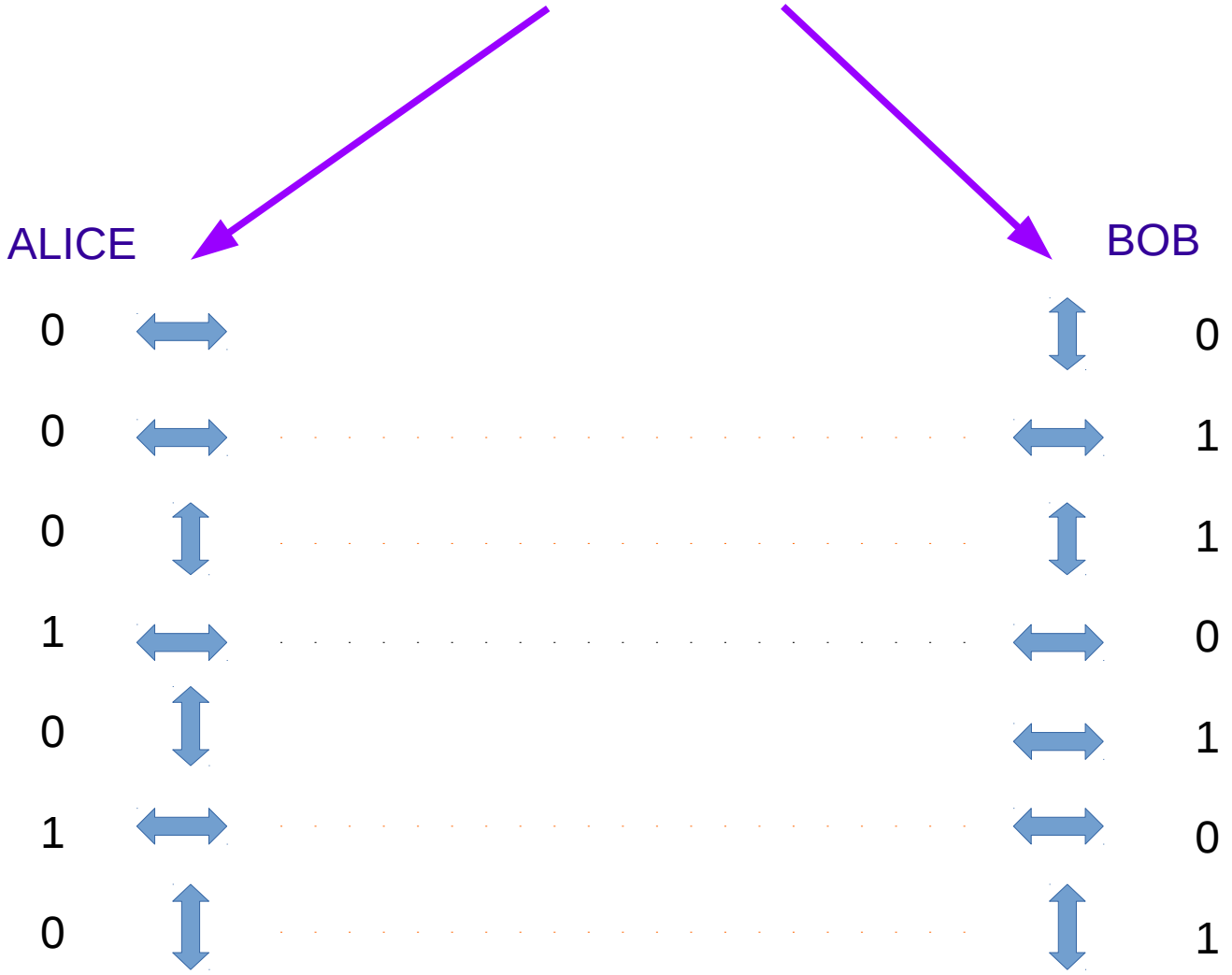


BB84: man in the middle attack



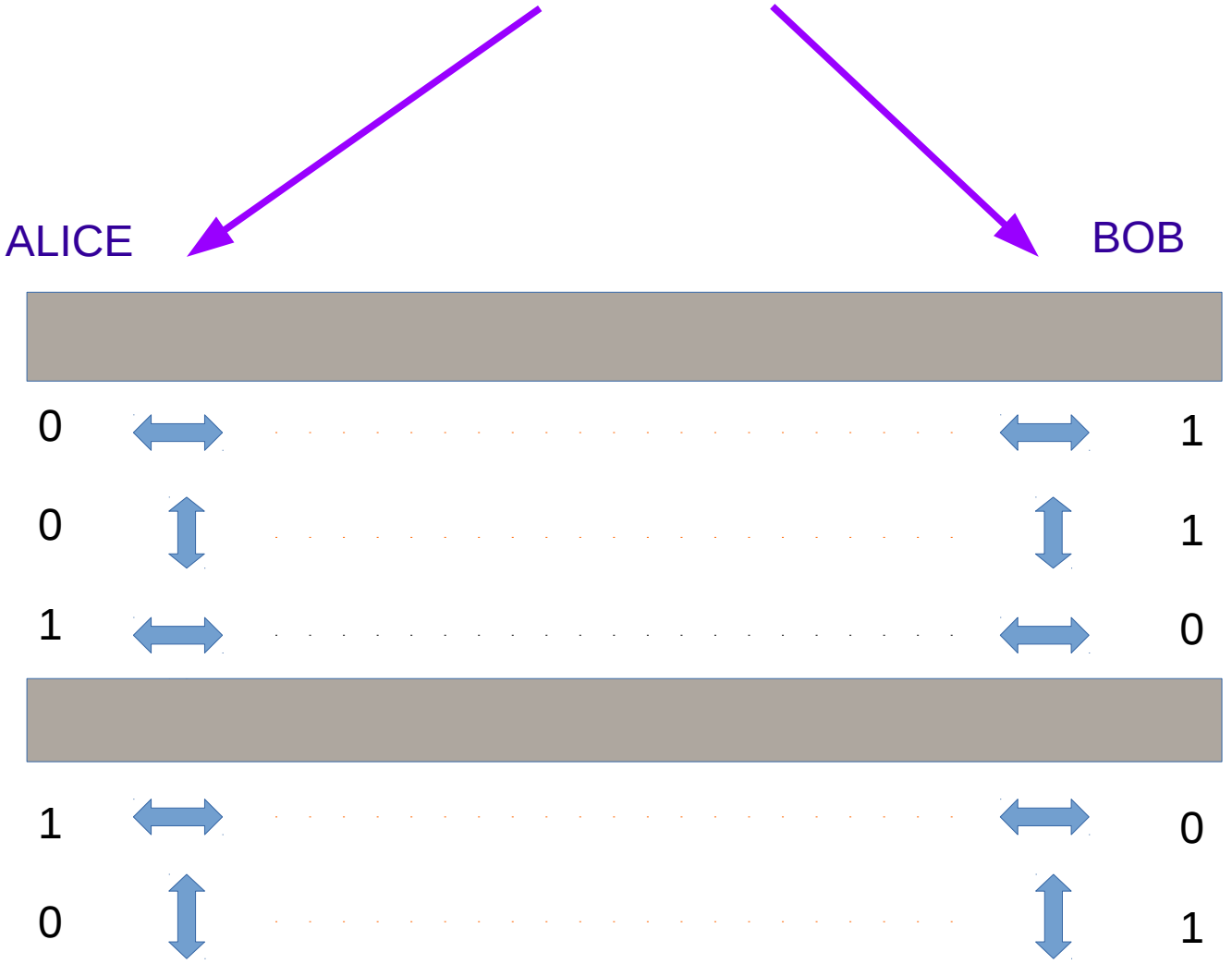
EKERT91

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



EKERT91

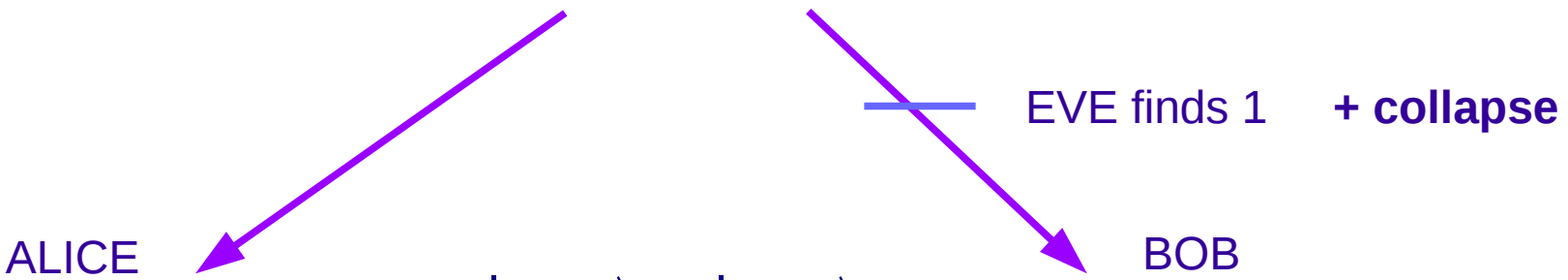
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01-10\rangle$$



ALICE and BOB share a secret key

EKERT91

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

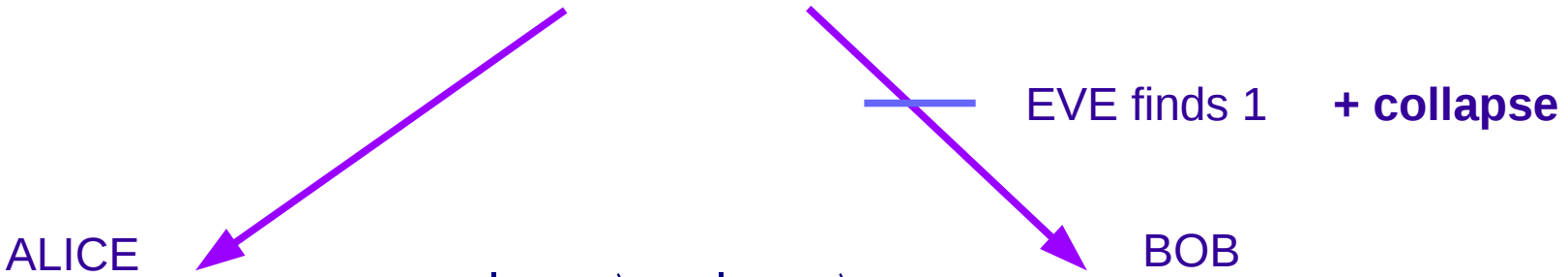


$$|\psi'\rangle = |01\rangle$$

How to detect EVE?

EKERT91

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



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

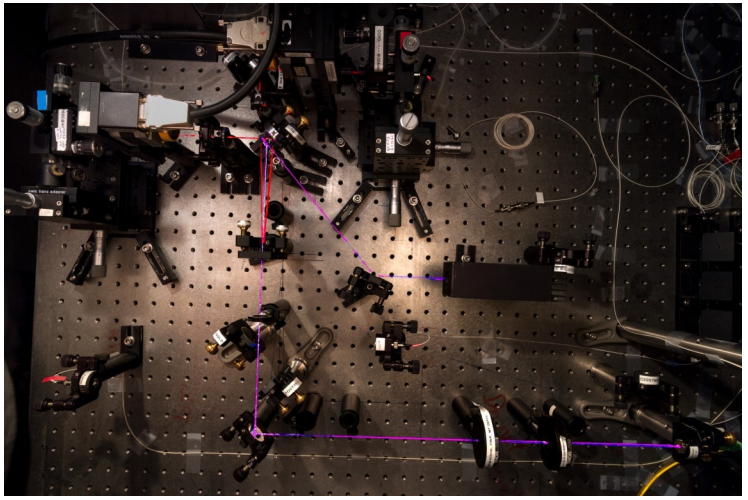
Alice and Bob measure Bell inequalities

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

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

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