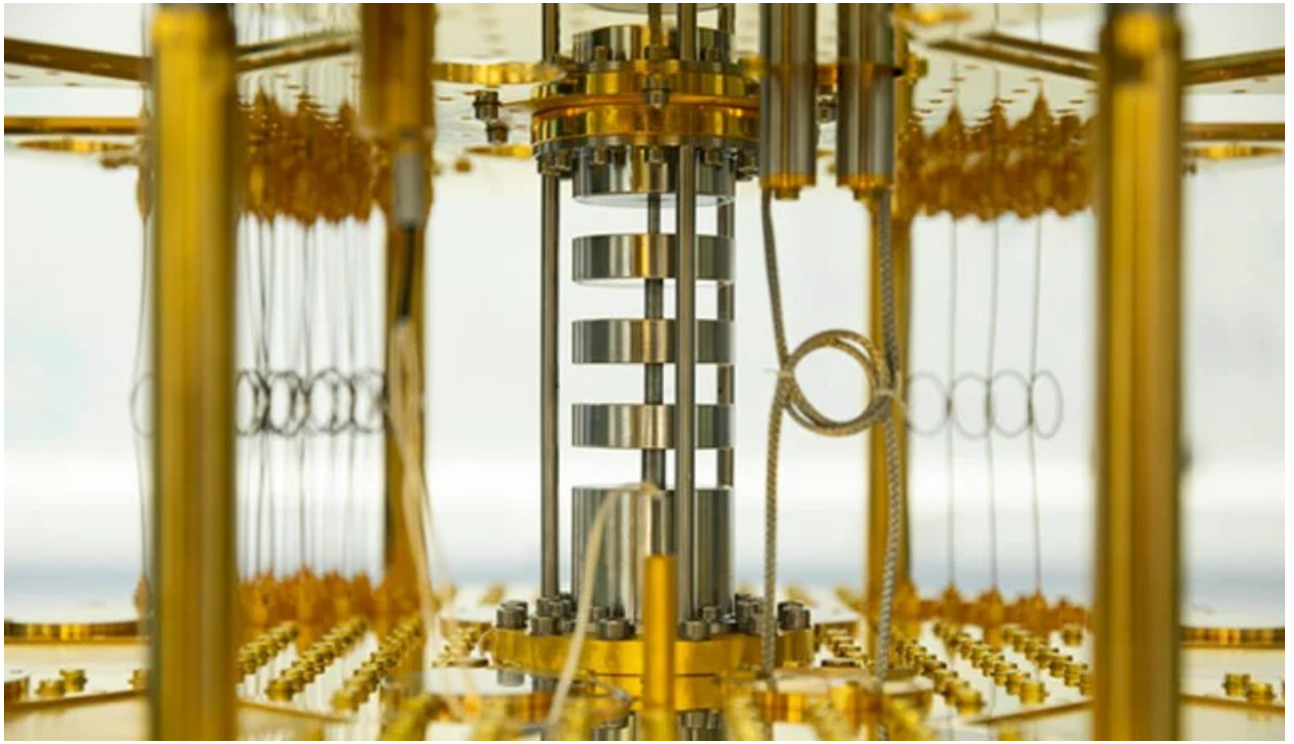
Quantum Computation

Infieri, September 2021

José Ignacio LATORRE

CQT, Singapore / TII, Abu Dhabi / Qilimanjaro, BCN



Computing
with
Quantum Mechanics

QM ➡ Information

Von Neumann & Copenhagen interpretation

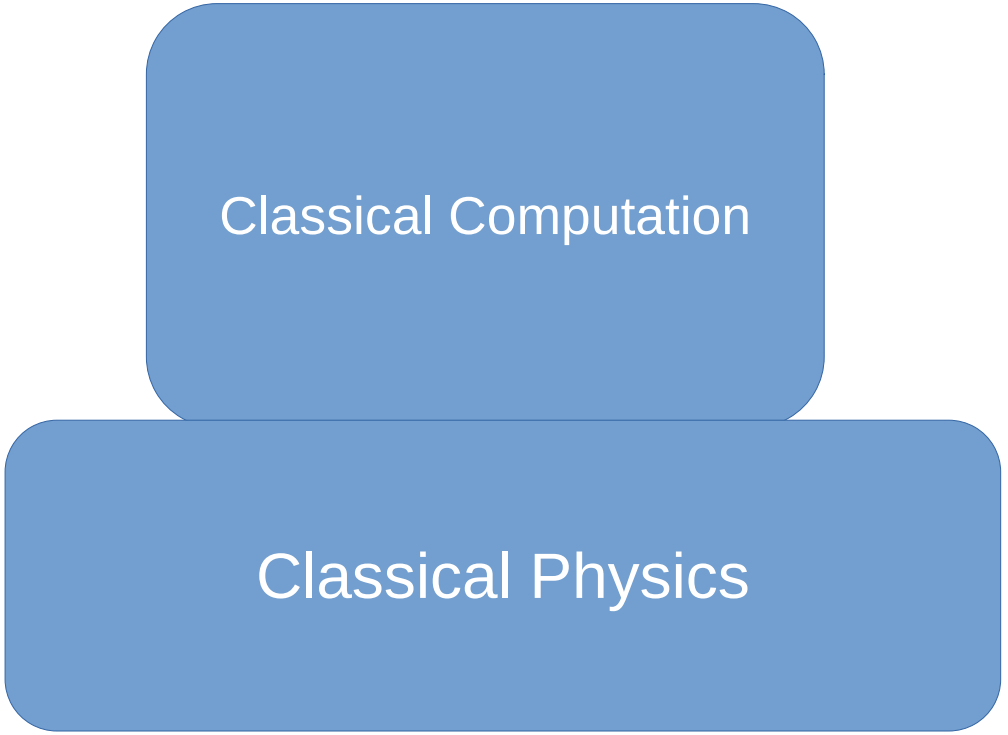
Postulate I
Ket keeps all available information on a system

Postulate II
Observables are related to operators acting on kets

Postulate III
Measurement collapses information
Born rule dictates this probabilistic collapse

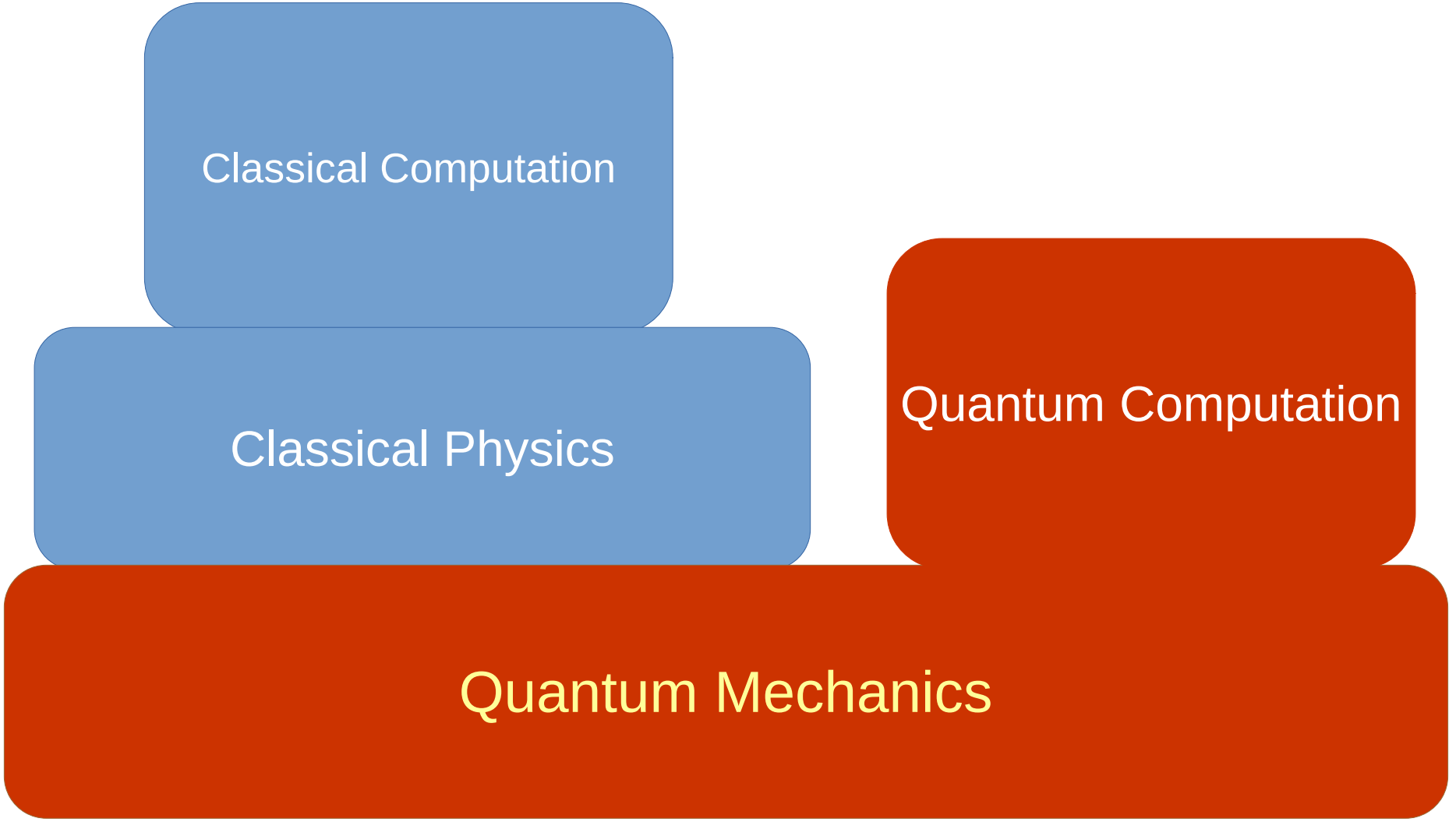
Postulate IV
Evolution is unitary and deterministic, keeps probabilities

Information ➡ QM



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

Information ➡ QM

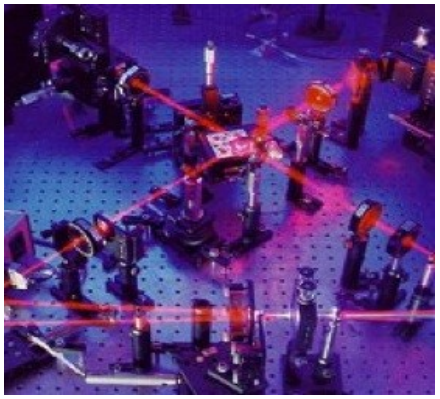


Feynman: Computing with QM

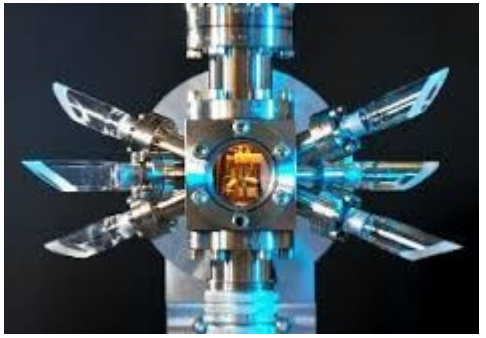
Physical implementations

Quantum Cryptography

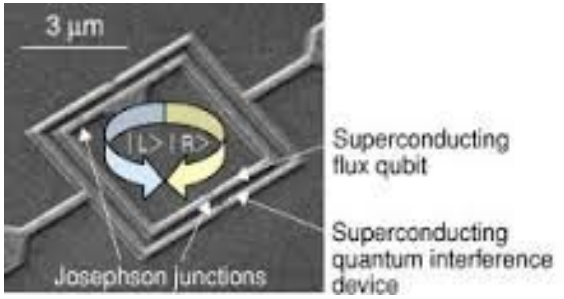
Quantum Computation



Photons:
H-V polarization
Time bins



Trapped ions:
ground-excited energy



Superconducting curents:
Left-right rotation

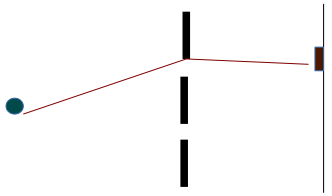
Superposition = QUBIT

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

(

Superposition

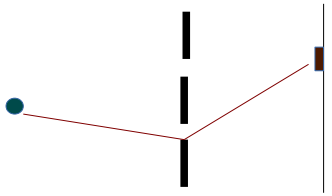
The information on a system may be on a ***superposition*** of various possibilities



$$|\psi_1\rangle$$

Superposition

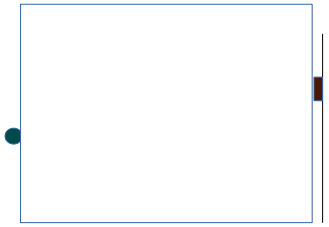
The information on a system may be on a ***superposition*** of various possibilities



$$|\psi_2\rangle$$

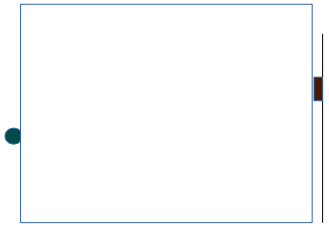
Superposition

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



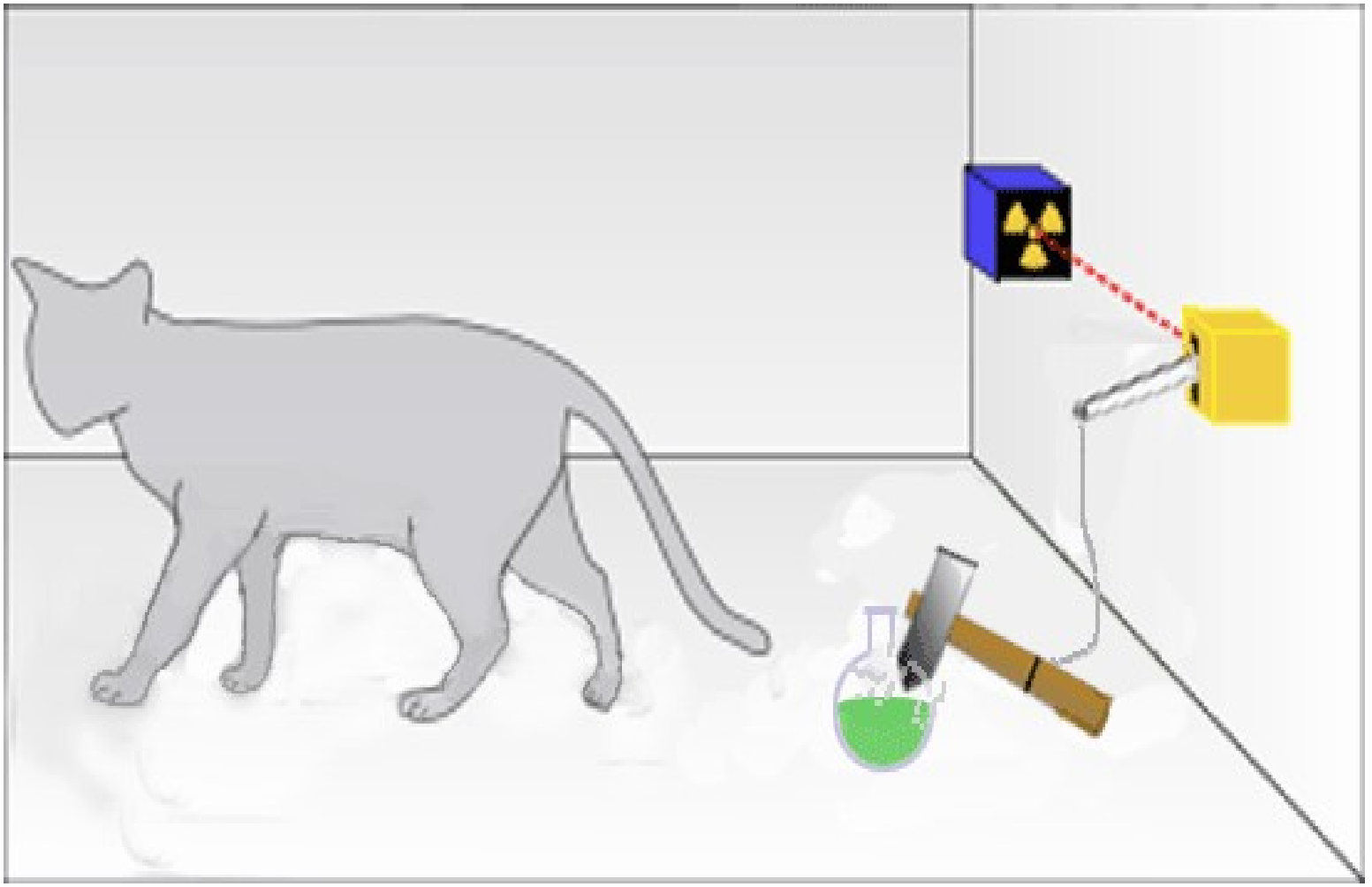
Superposition

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

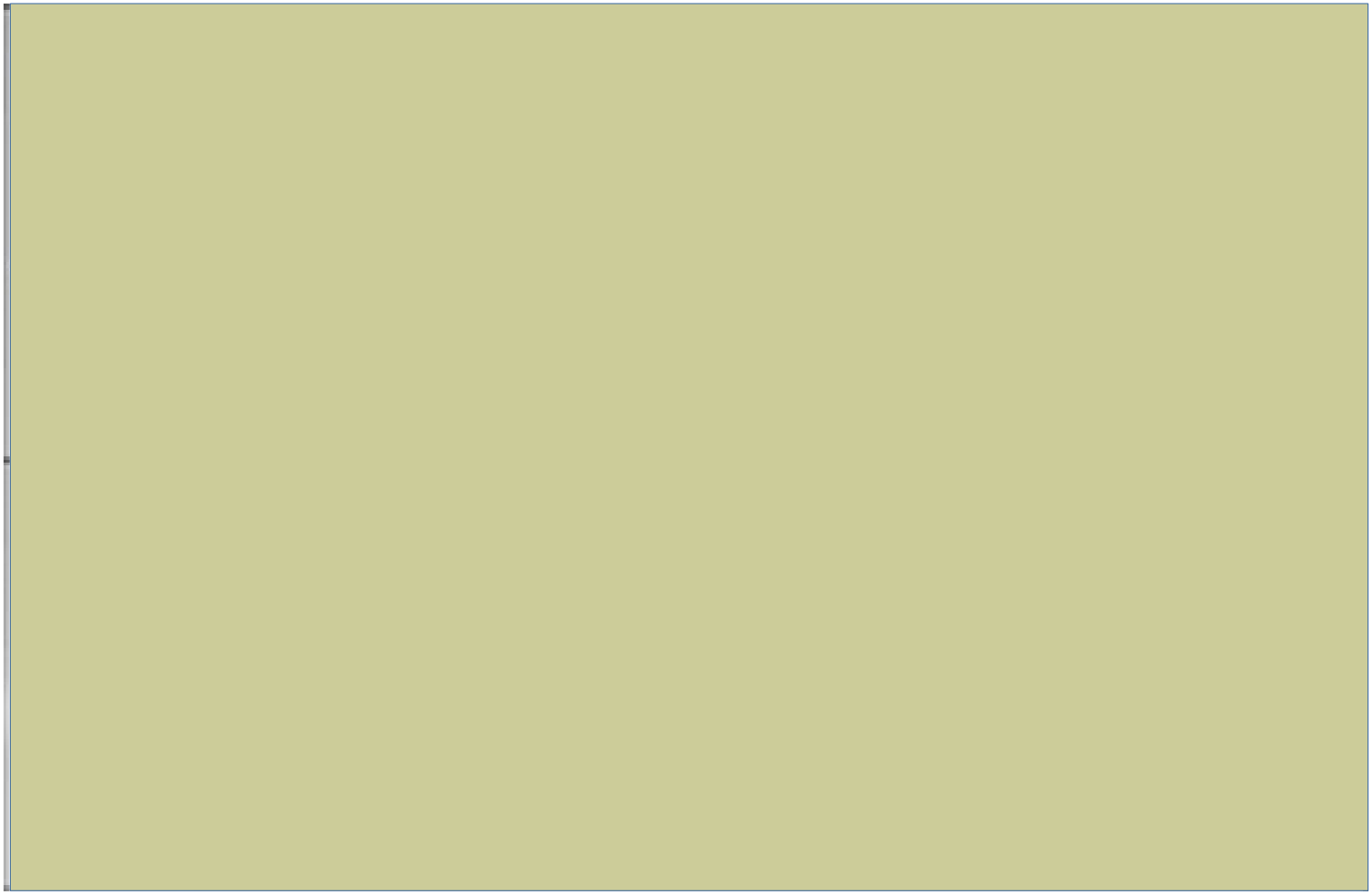


$$|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$$

Schrödinger's cat



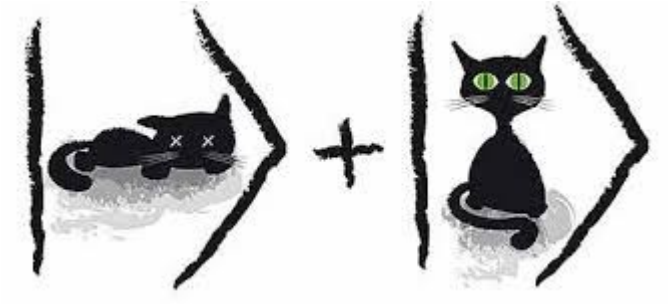
Schrödinger's cat



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."

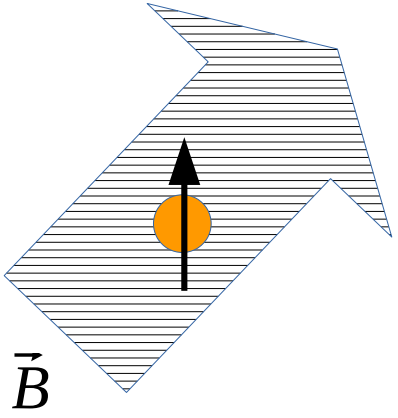
Let's use quantum superposition to codify information

We can codify arbitrary superpositions of logical bits: QUBIT

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

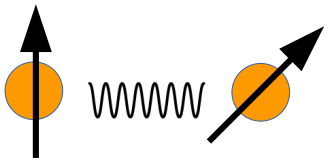
)

Unitary Evolution = Quantum Gates



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

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



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

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

Physical interaction = Q 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!

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

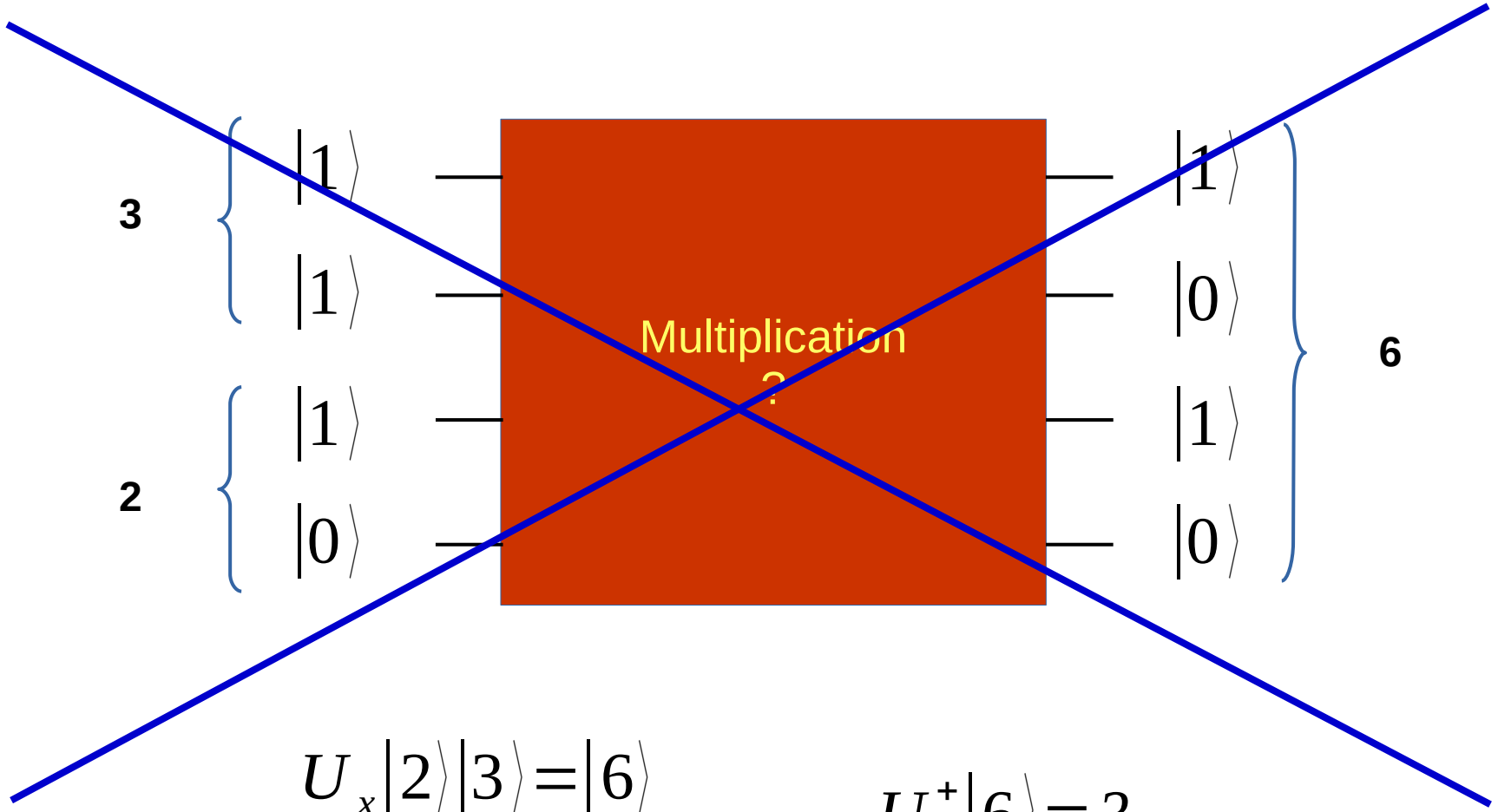
BUT

Quantum Mechanics follows its on laws

Multiplication

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

Multiplication

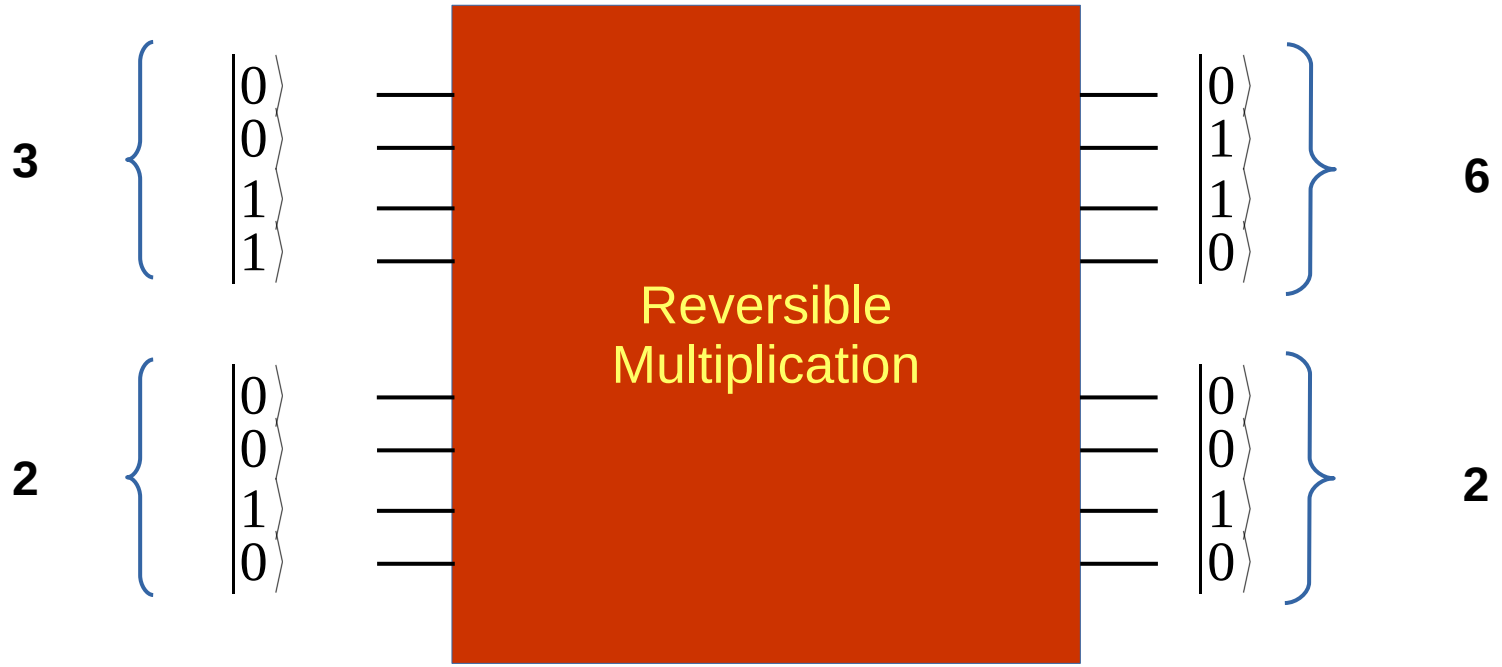


$$U_x|2\rangle|3\rangle=|6\rangle$$
$$U_x|1\rangle|6\rangle=|6\rangle$$

$$U_x^+|6\rangle=?$$

NOT UNITARY

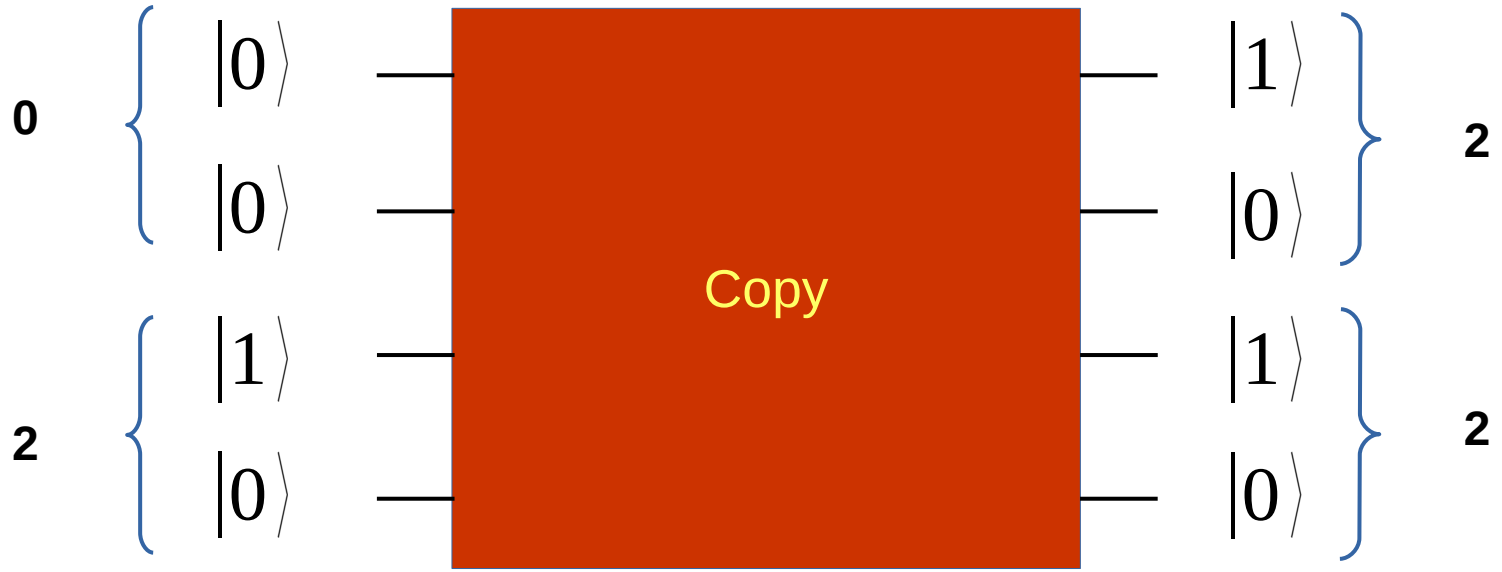
Unitarity = Reversible Computation



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

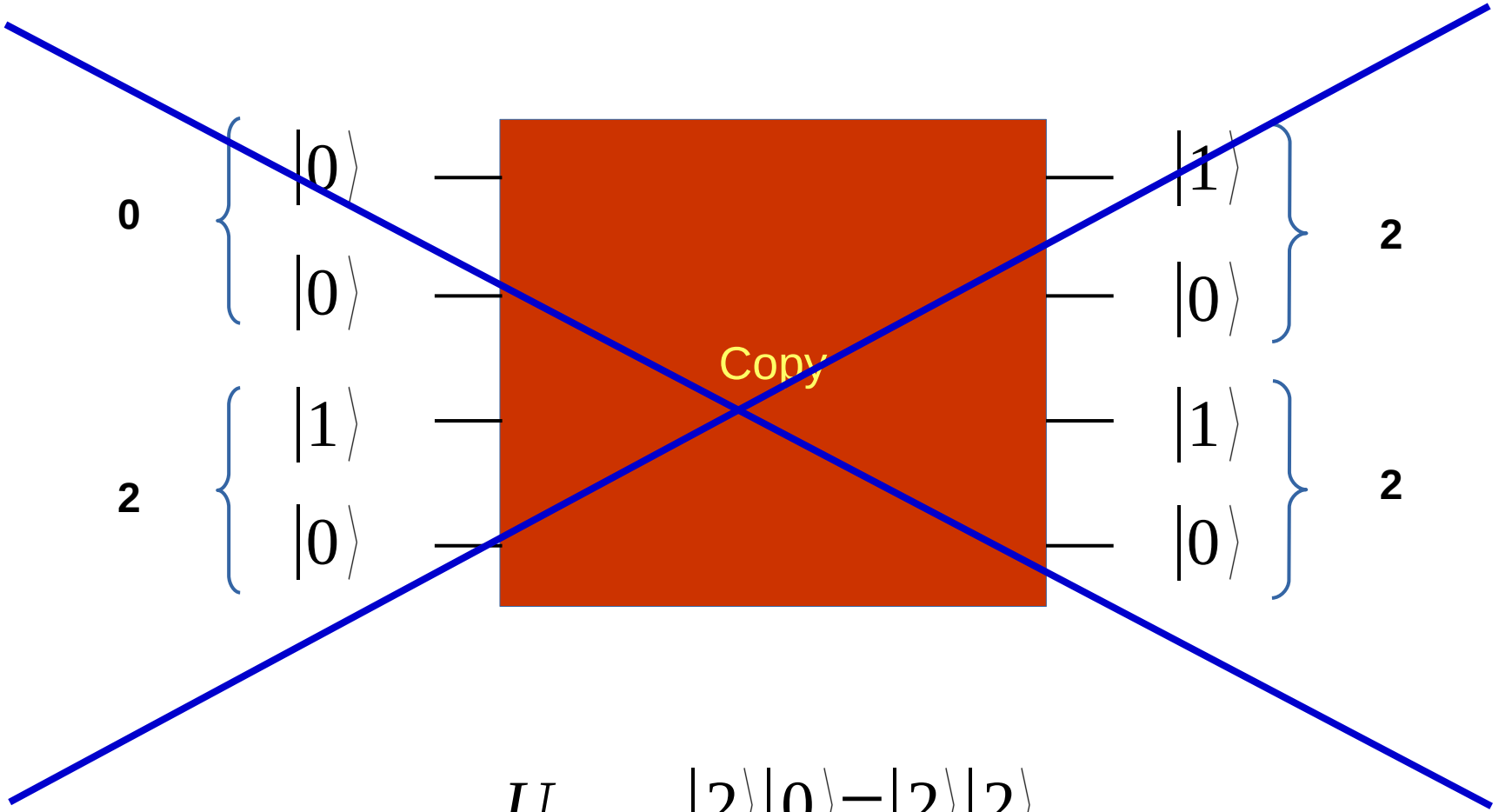
$$U_x|x\rangle|y\rangle = |x\rangle|f(x,y)\rangle$$

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

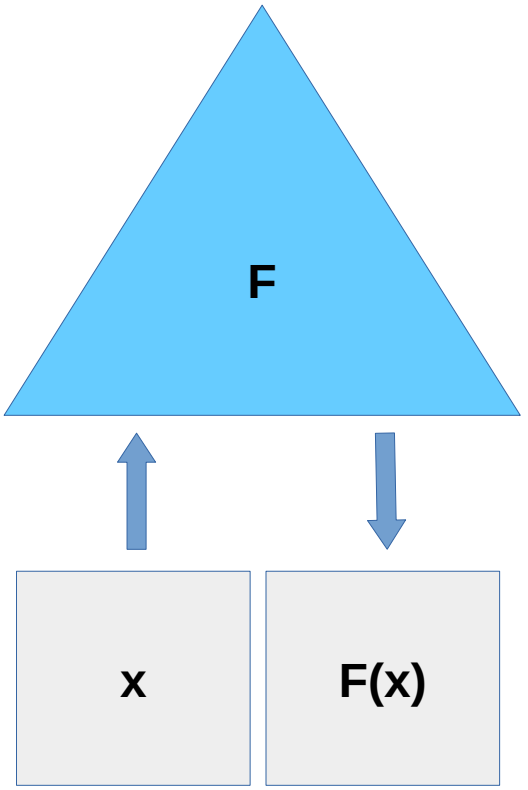
$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} \left| i_1, i_2, \ldots, i_n \right\rangle$$

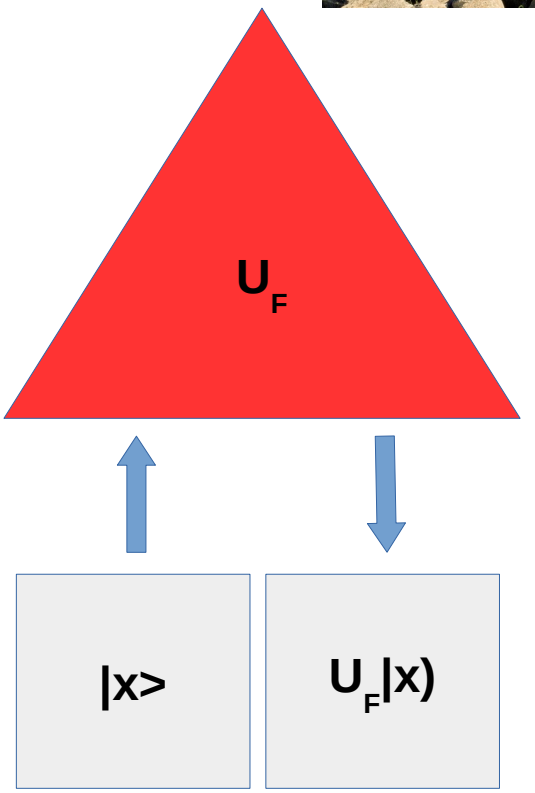
$$P\left(i_1, i_2, \ldots, i_n\right) = \left| c_{i_1, i_2, \ldots, i_n} \right|^2$$

The magic of

Quantum Algorithms

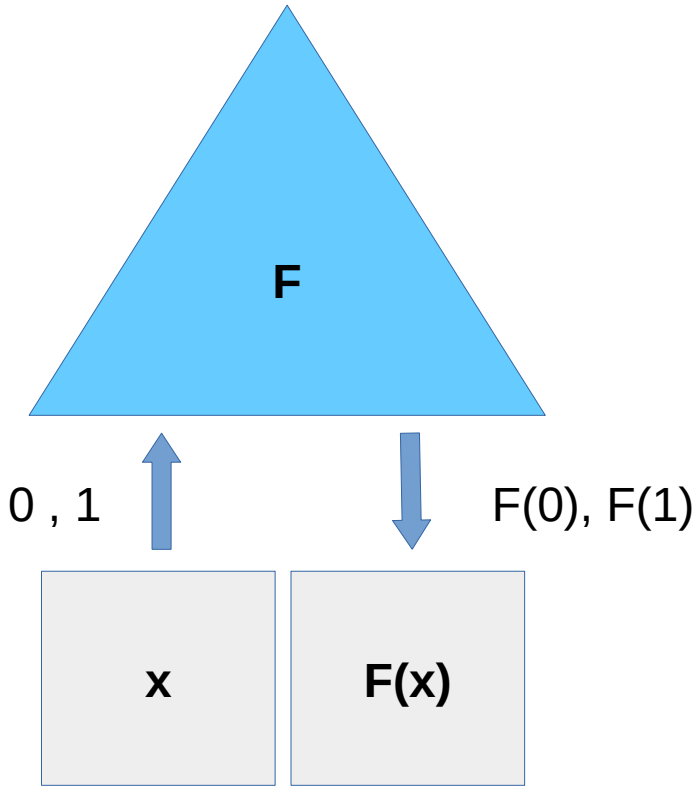
Queries to an **oracle**





Can QM reduce the number of calls to an oracle?

Queries to an **oracle**



Simplest example: is F constant?

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

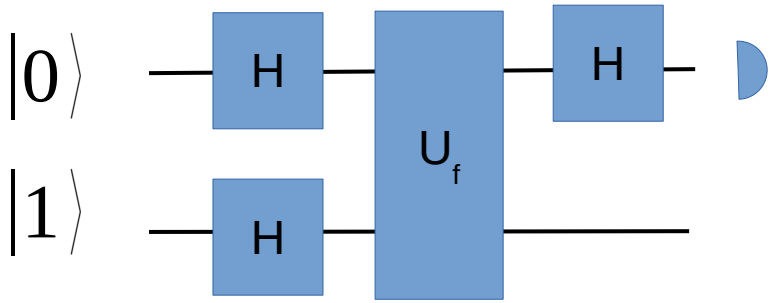
$$F(0)=F(1)\,?$$

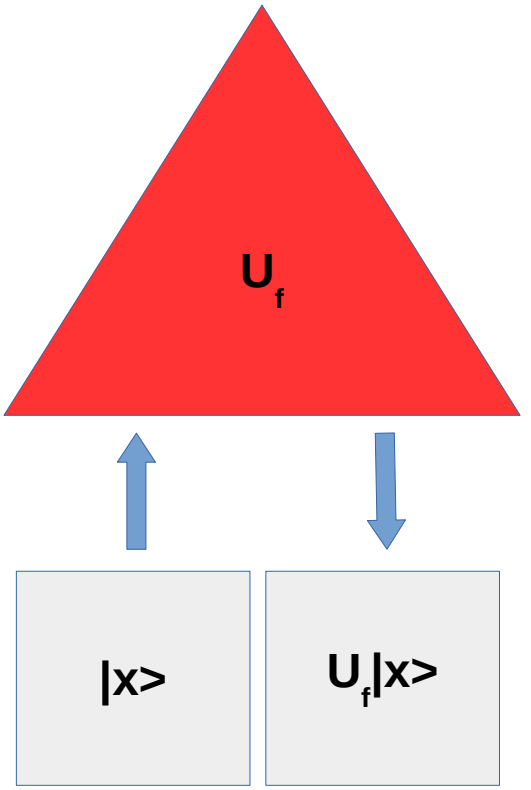
$$F(0)\neq F(1)\,?$$

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

Queries to an **oracle**

Deutsch–Jozsa





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

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

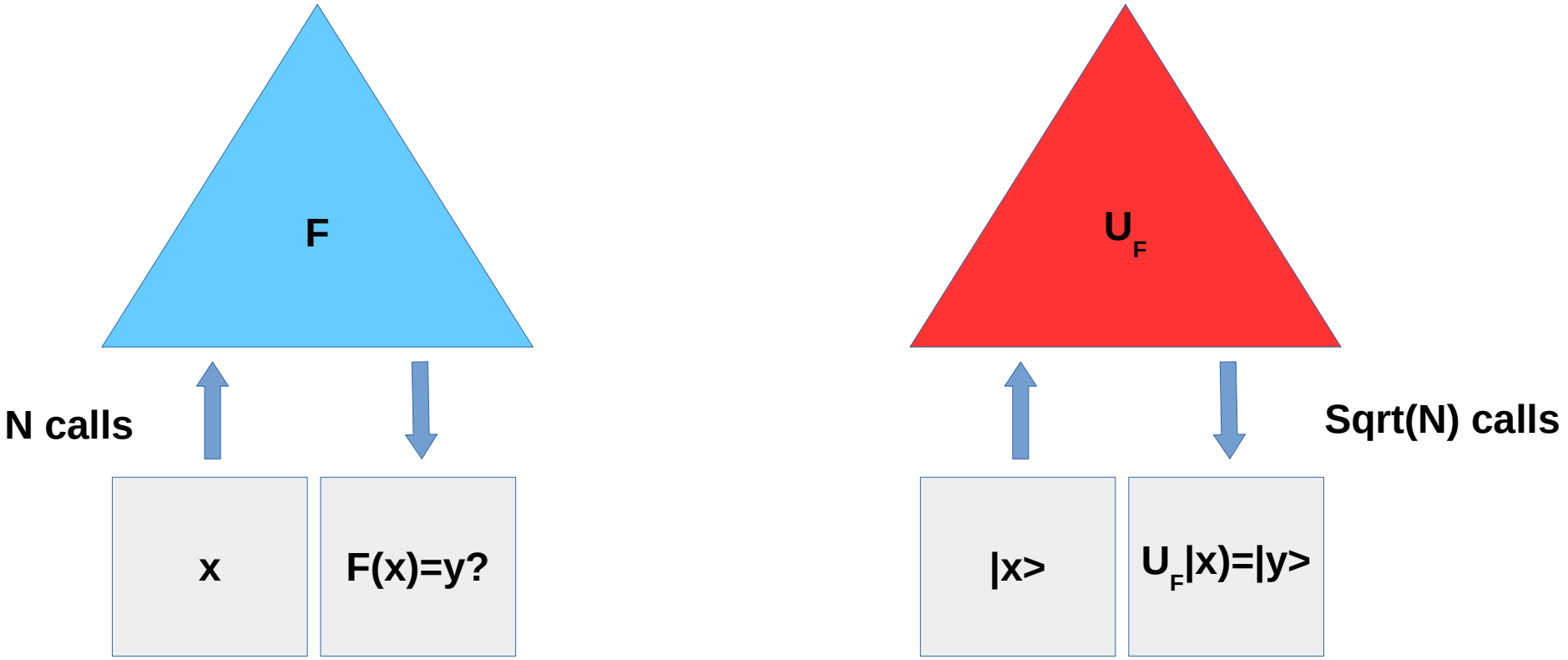
$$|0\rangle(|0+f(0)\rangle-|1+f(0)\rangle)+|1\rangle(|0+f(1)\rangle-|1+f(1)\rangle)$$

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

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

QM needs a single call to the oracle!!

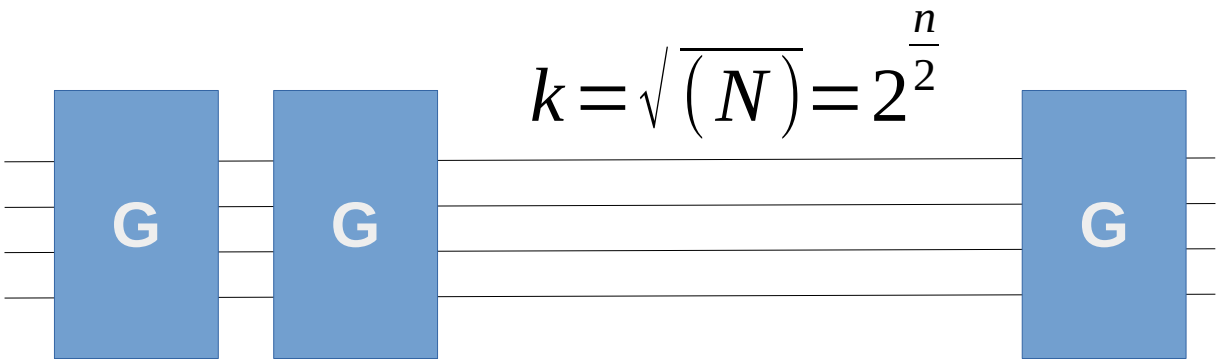
Queries to an oracle: **search an unstructured database**



Grover's algorithm

Solve a hash, bitcoin! Applications to many fields.

Grover Algorithm



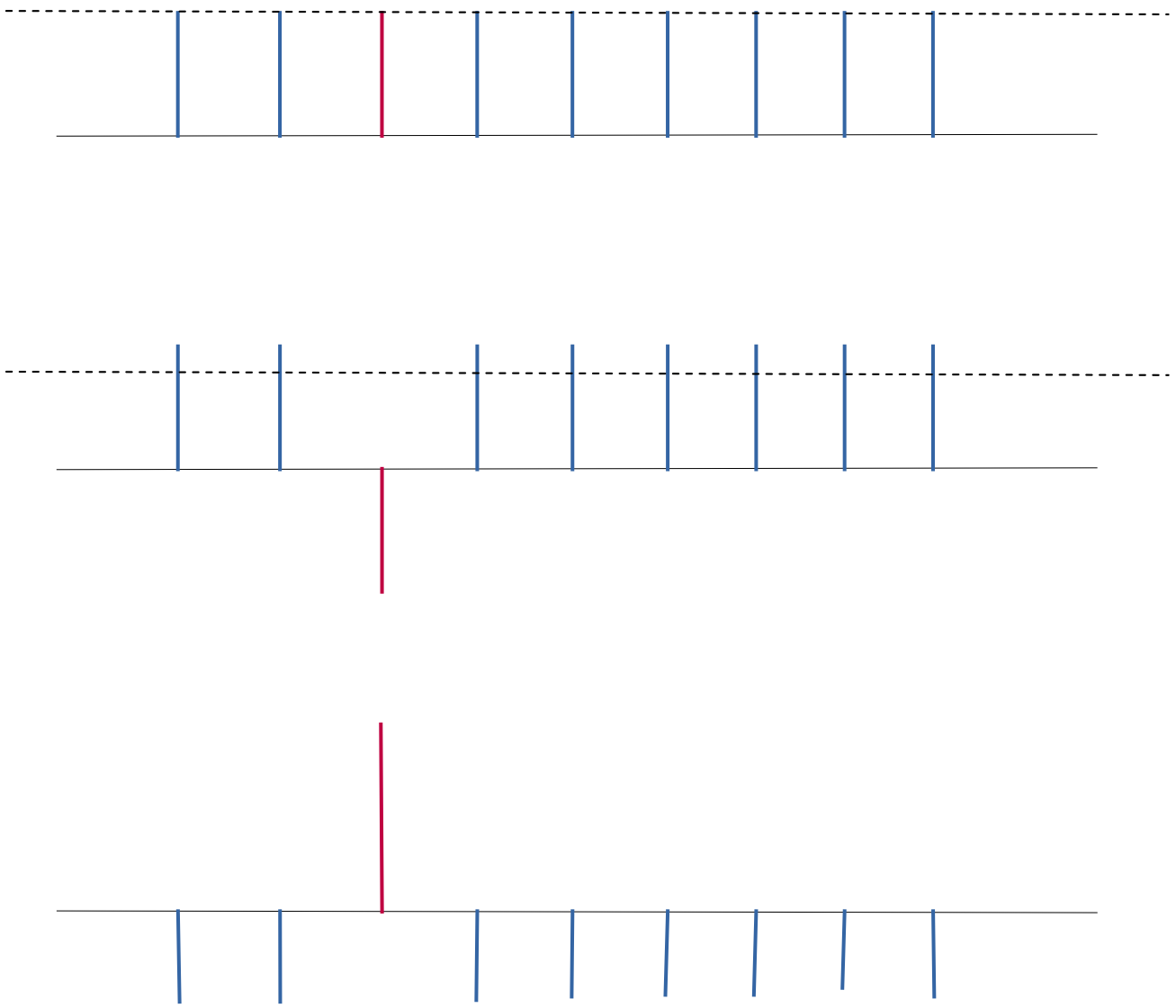
Search space: $N=2^n$

G $= U_f U_s$

$$U_f = 1 - 2|w><w|$$

$$U_s = 1 - 2|s><s|$$

$$|s\rangle = \frac{1}{\sqrt{(N)}} \sum_x |x\rangle$$



Probability is transferred coherently from the rest of states to the solution

Factorization

$$N = p\,q$$

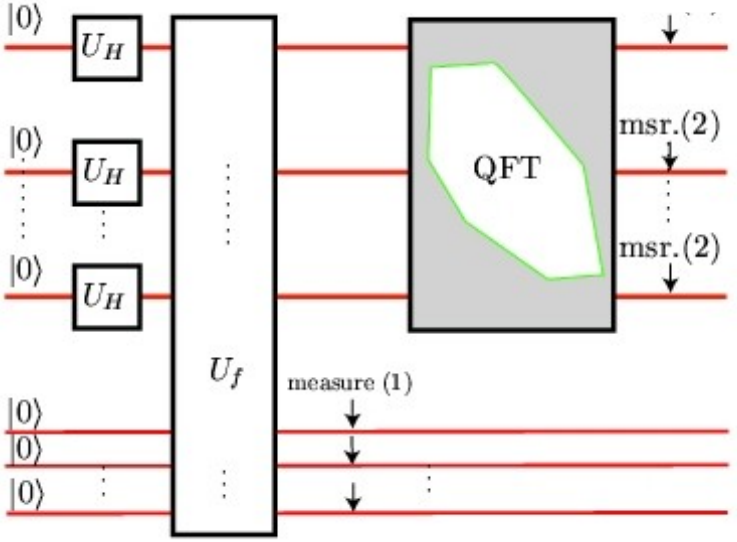
Choose a and find r such that $a^r = 1 \bmod(N)$

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

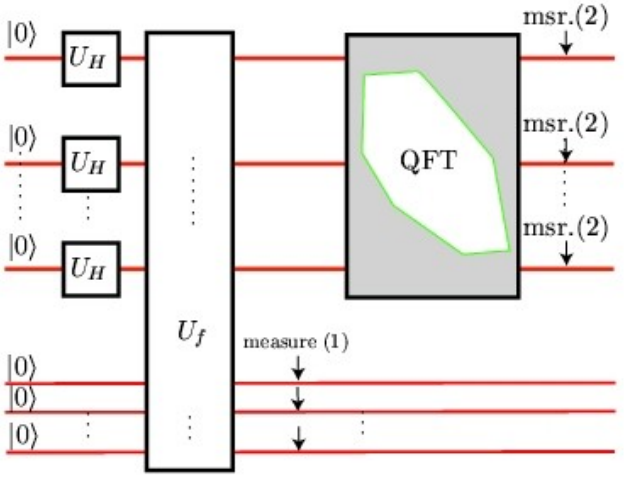
Factoring = Finding a hidden period

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

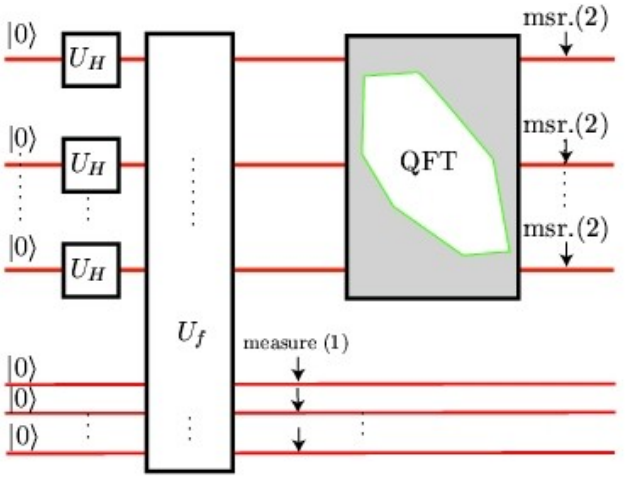


$$U_H\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

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

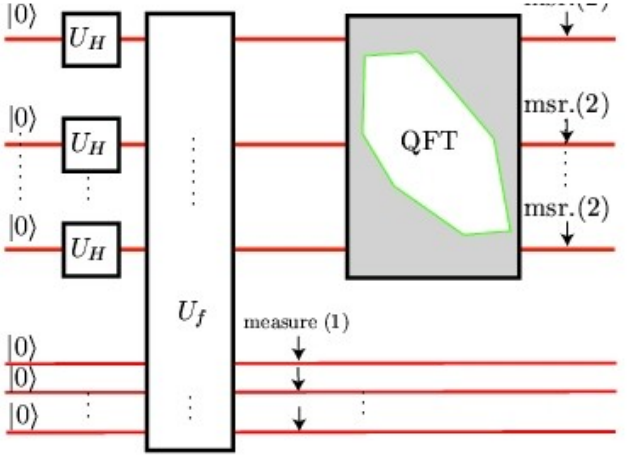


$$|\psi_3\rangle = U_f\,|\psi_2\rangle = \frac{1}{Q}\sum_{x=0}^{2^n-1} |x\rangle\,|a^x \bmod(N)\rangle$$



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

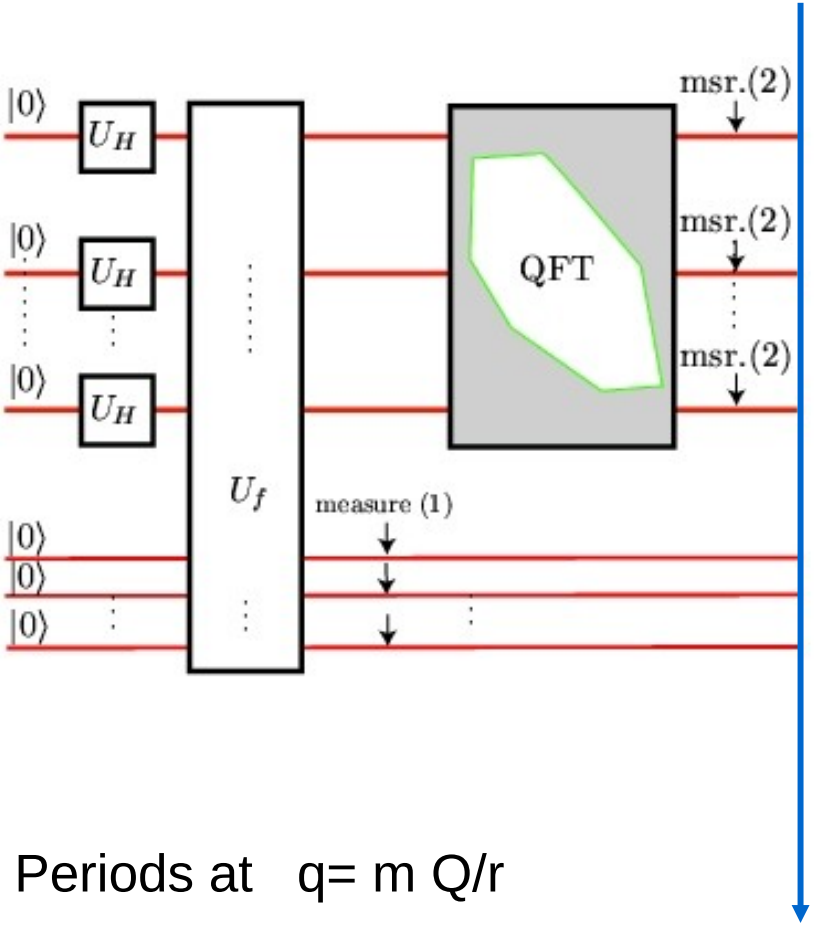
$$|\psi_4\rangle = \frac{1}{B}\sum_{k=0}^{B-1} |d_b + kr\rangle\,|b\rangle$$

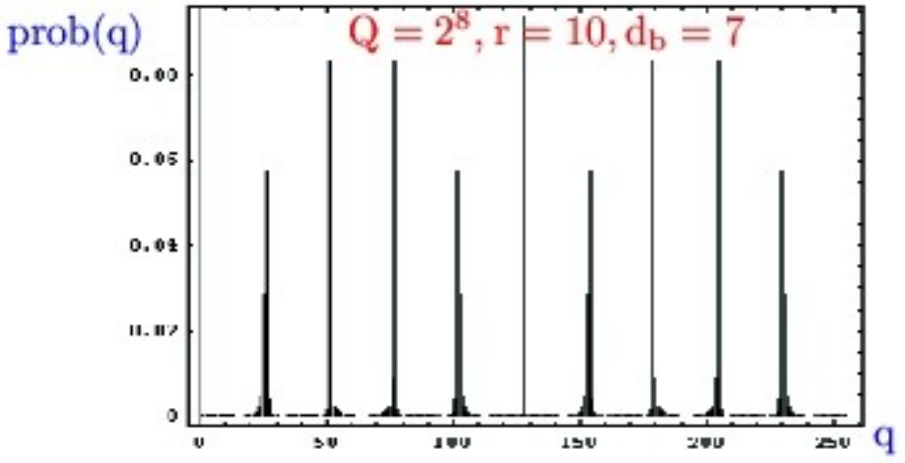


$$|\psi_5\rangle = \frac{1}{\sqrt{QB}} \sum_q \sum_k e^{iq2\pi(d_b + kr)} |q\rangle |b\rangle$$

Shor's algorithm

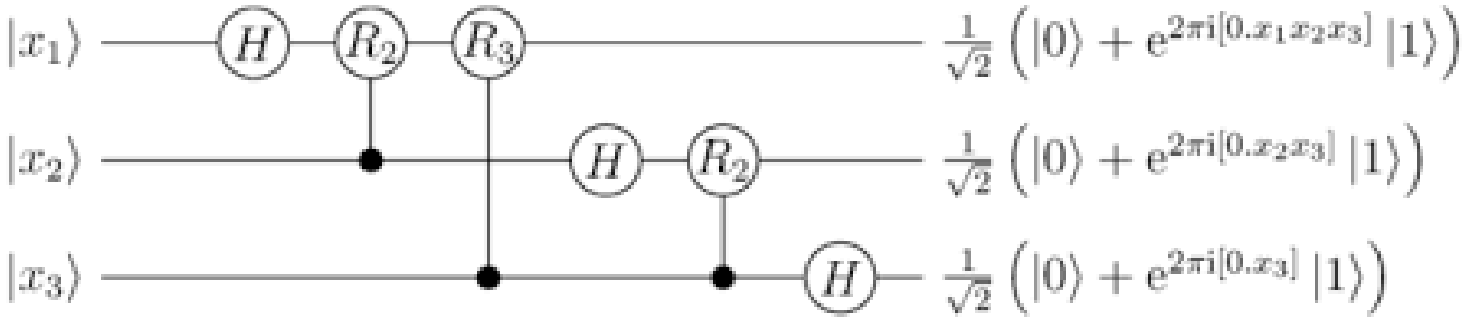
$$P(q) = \frac{1}{QB}\left|\sum_{k=0}^{B-1} e^{iqr\,2\pi/Q}\right|^2$$





Periods at q= m Q/r

read r



Quantum Fourier Transform is efficient!!!!! n^2

Applications

- Factorization
- Sincronization
- Amplitude Amplification
- ….

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, size 2n+3

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.

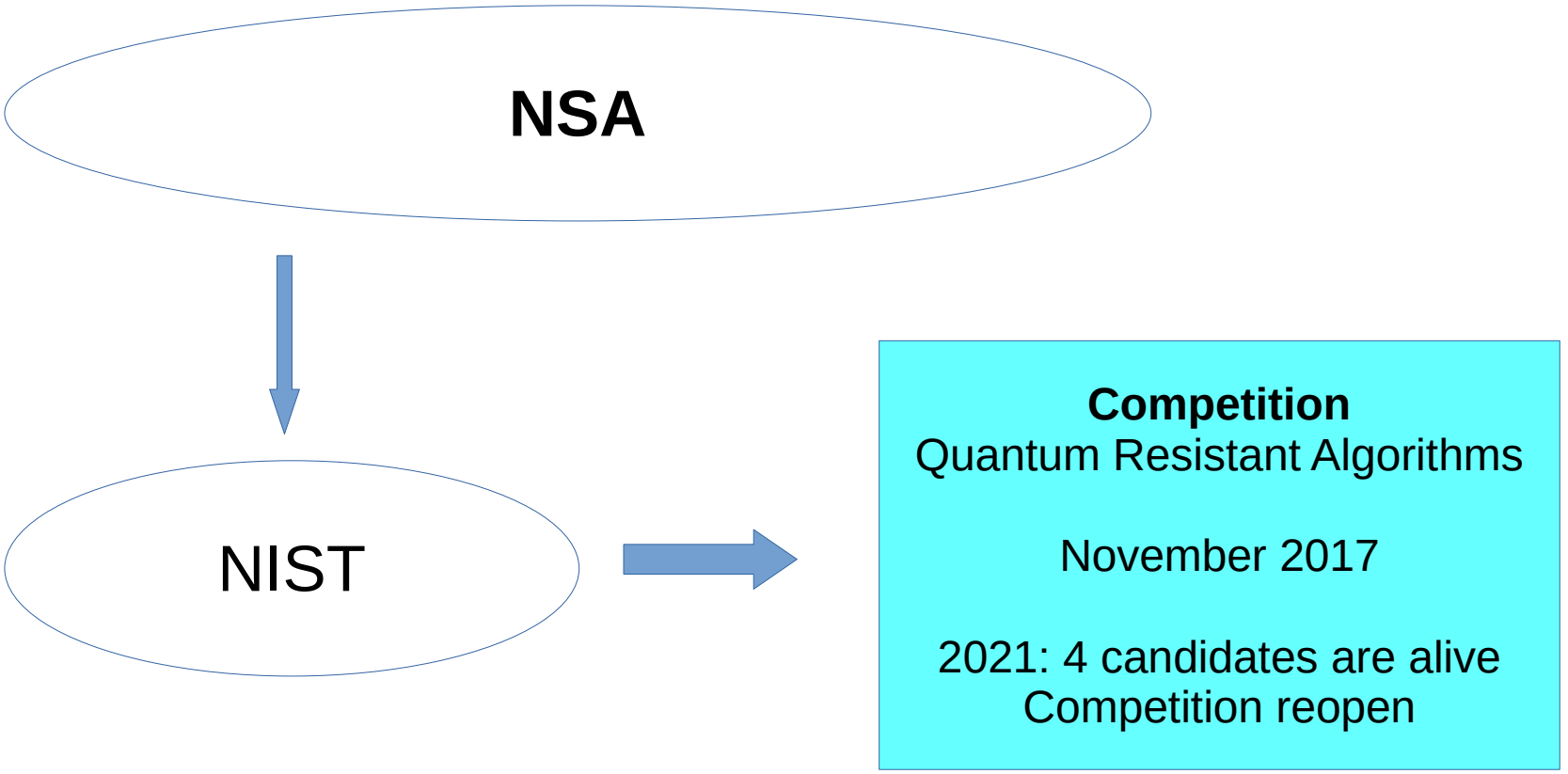
The NSA remarked that "The AES-256 and SHA-384 algorithms are symmetric, and believed to be safe from attack by a large quantum computer."

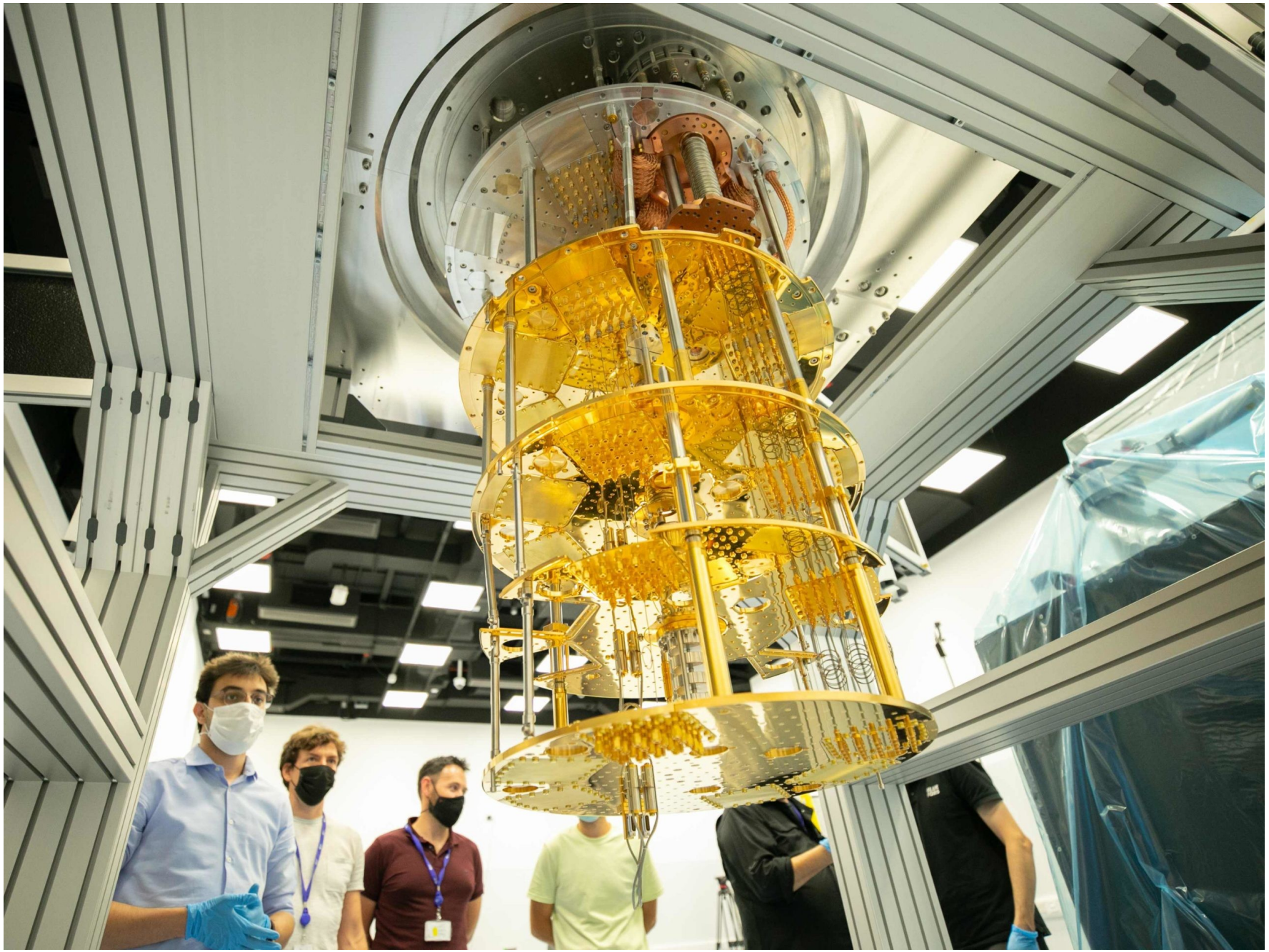
According the NSA, the following isn't safe to use:

- 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
2021: 4 candidates are alive
Competition reopen



To be Qontinued!