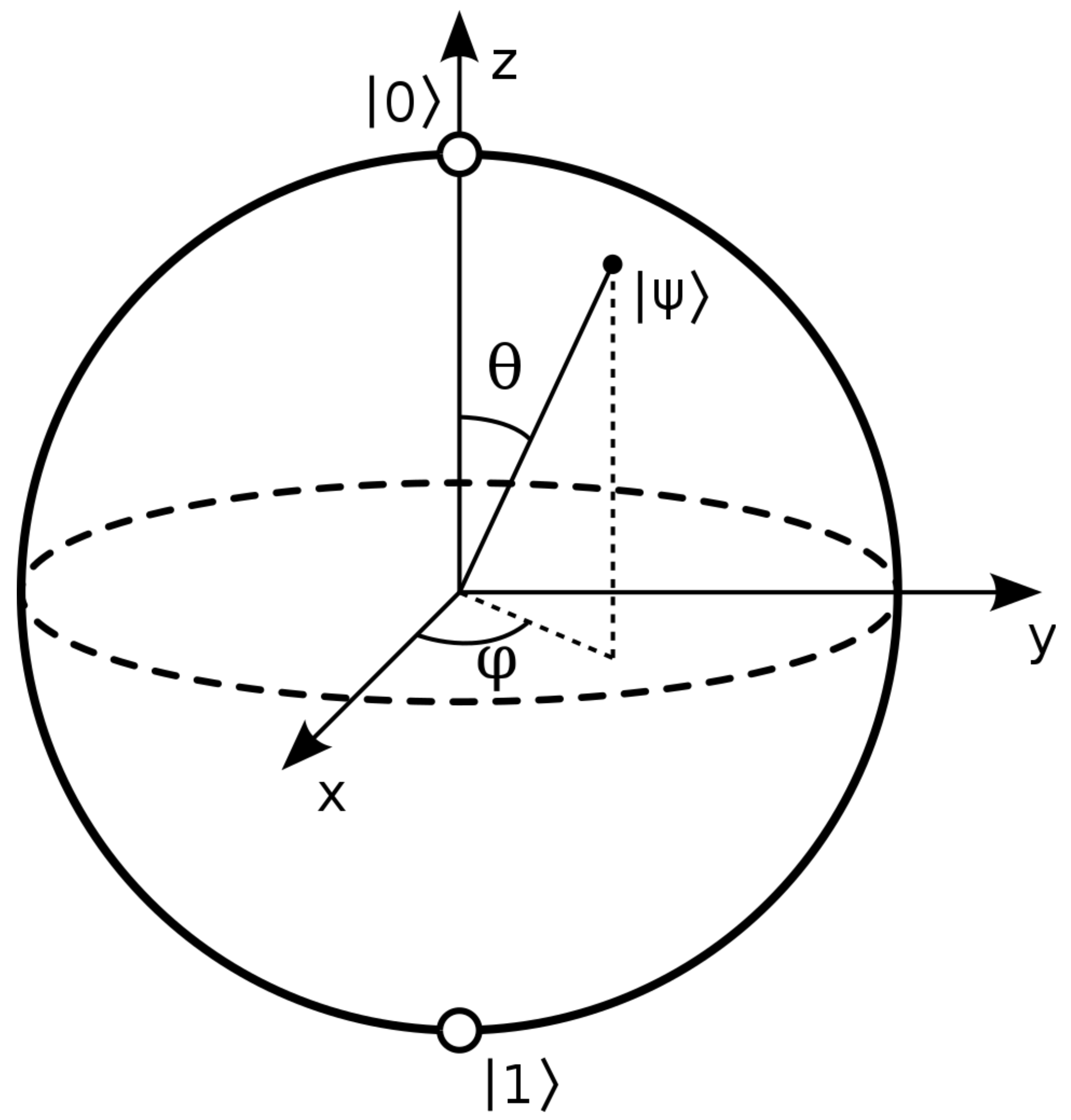
QuBit Conference

QuBit Conference
PRAGUE 2019

Evil Qubits
The Threat of Quantum Cryptanalysis Explained

Tomas Rosa
Raiffeisen BANK International Cryptology and Biometrics Competence Centre

Postulate #1: Qubit state belongs to Hilbert space of dimension 2



$$|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right),\ \omega_i \in \mathbb{C}$$

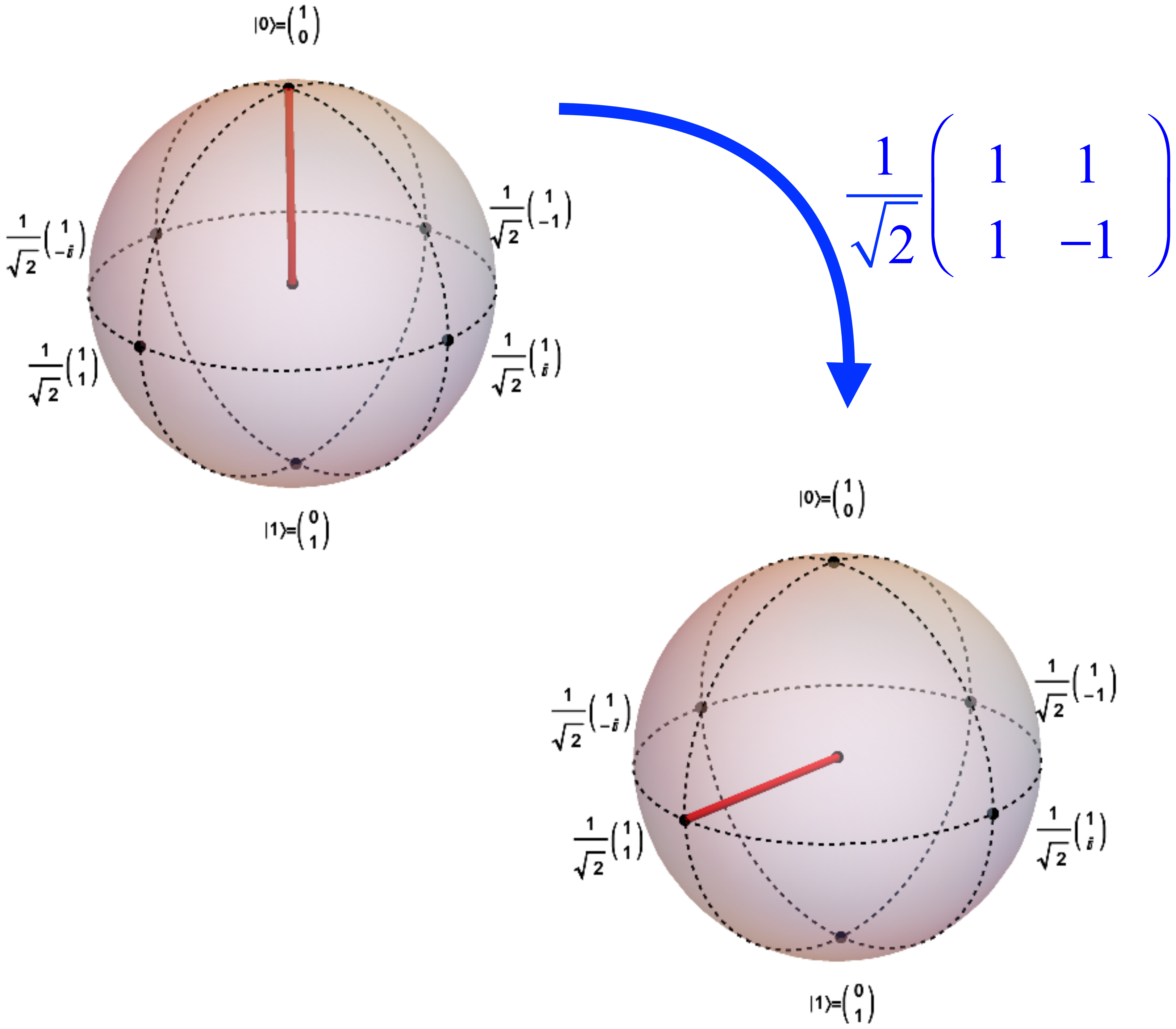
$$|\omega_0|^2 + |\omega_1|^2 = 1$$

Postulate #2: Qubit evolution is given by a unitary transformation

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H|\psi\rangle$$

$$\boxed{|\psi_t\rangle = U_t |\psi_{t_0}\rangle, \; U_t = e^{\frac{-iHt}{\hbar}}}$$

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \ldots$$



Postulate #3: Projective probabilistic measurement

- When measured, quantum state collapses into one of particular eigenstates comprising the basis vectors of the corresponding Hilbert space.
- For a qubit, these are labeled **|0>** and **|1>**. So called computational basis.
- Superposition cannot be seen directly. It governs the probability of the measurement outcome; coefficients ω_i called ***probability amplitudes***.

$$P[result = |i\rangle] = |\omega_i|^2 = \omega_i \cdot \omega_i^*$$

Postulate #4: Qubit register state belongs to $\boldsymbol{H}_2 \otimes \boldsymbol{H}_2 \otimes \ldots \otimes \boldsymbol{H}_2$

- Exponencial growth of dimension: n-qubit register belongs to Hilbert space of dimension 2^n and can be in a superposition of all of its 2^n eigenstates.

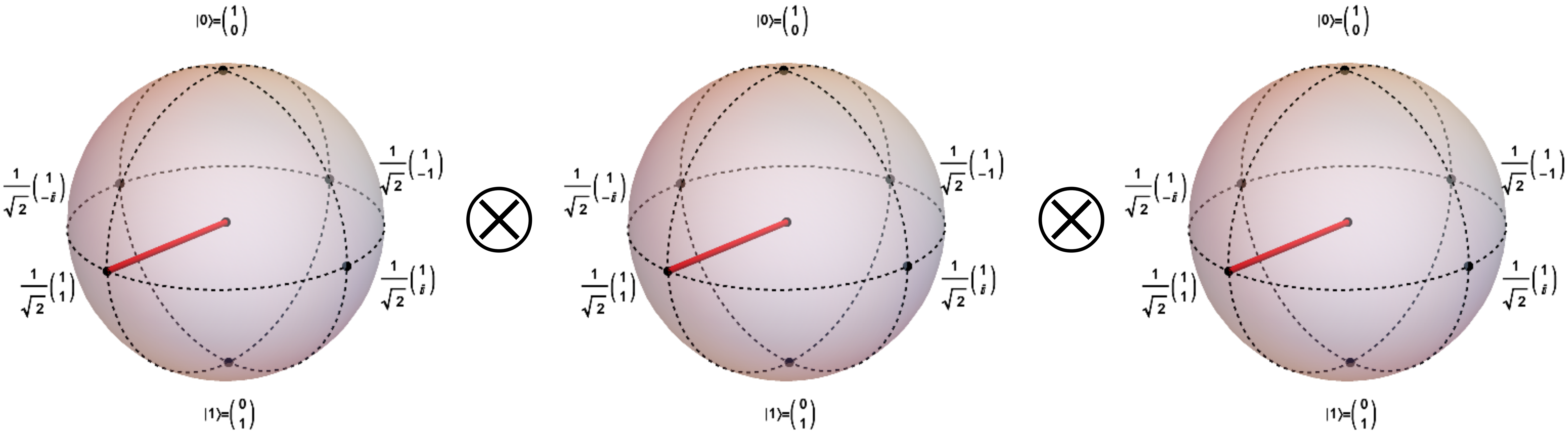
  - together with linear operators acting on this register, this is the source of so-called **quantum parallelism**

  - however, the superposition still cannot be seen directly, it still just governs the probability of the measurement outcome

  - eigenstates (computational basis) **|00…0>**, **|00…1>**, …, **|11…1>**

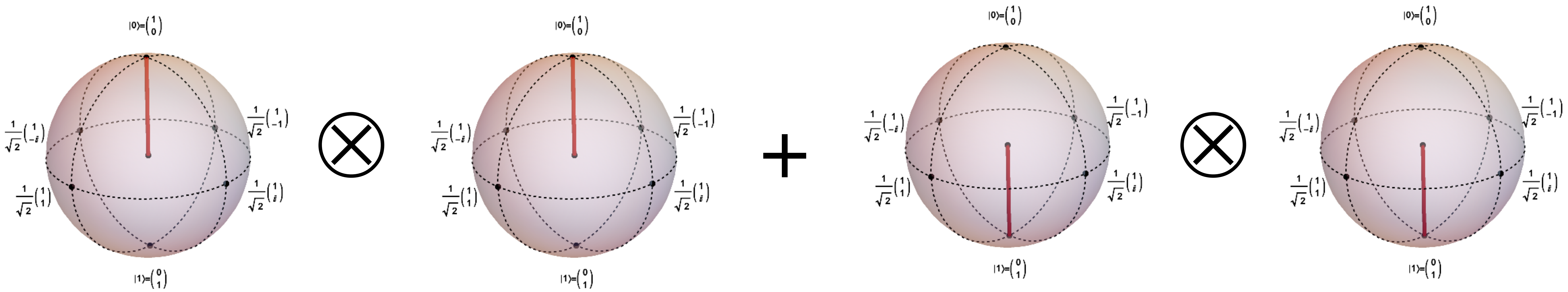
  - sometimes, the tensor product is noted explicitly |00…0> = |0>|0>…|0>, etc.

Separable Register State Example (Note the Pure Tensor Product…)



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

Entanglement (Note the Unavoidable Sum of Tensor Products…)



$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Computational Aspects

- Actually, we have already reformulated the quantum mechanics postulates slightly to tailor them to qubits and qubit registers.

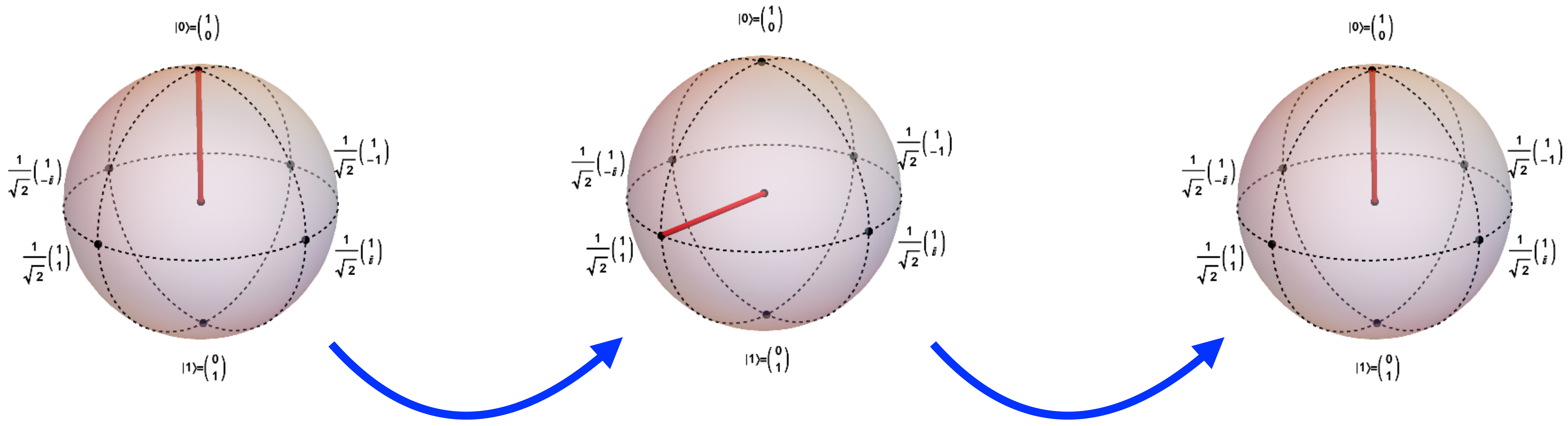
- We can continue further to derive computational paradigms. For instance:

  - quantum parallelism (already noted above)

  - interference (constructive / destructive, enabled by the complex amplitudes)

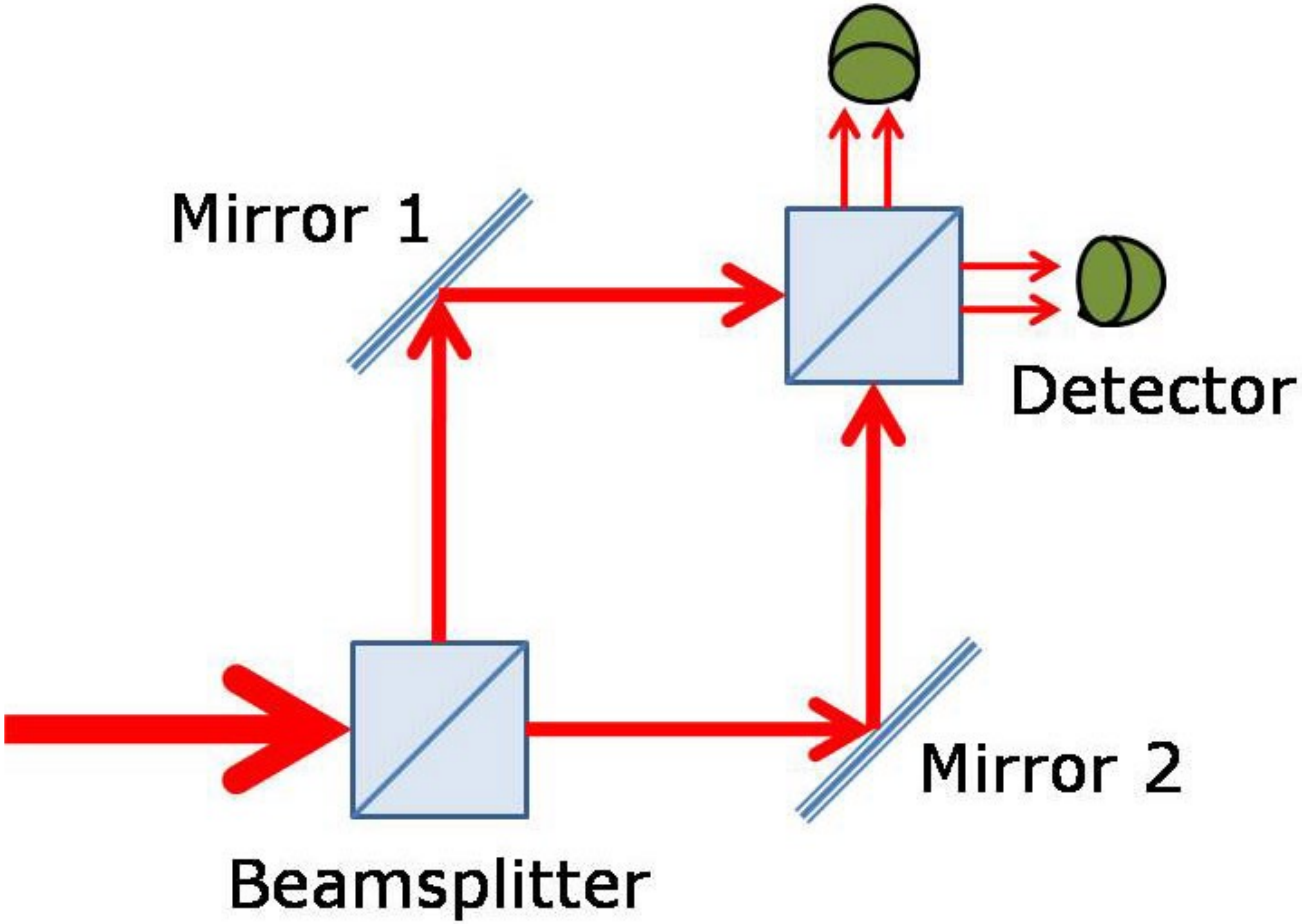
  - entangled states (seen as an extra power for algorithms)

Computational Interference



$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

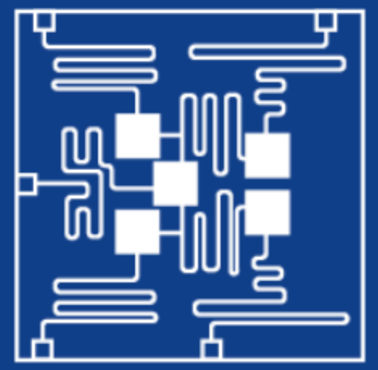
This was just a computational version of Mach-Zehnder experiment

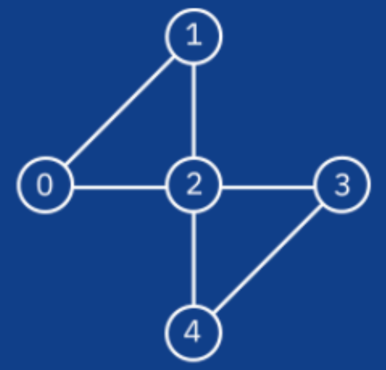


Time to Say: “Hello World!”

IBM Q 5 Tenerife [ibmqx4]

ACTIVE: USERS





Last Calibration: 2019-02-28 03:58:10

	Q0	Q1	Q2	Q3	Q4
Frequency (GHz)	5.25	5.30	5.35	5.43	5.18
T1 (μs)	47.80	57.00	48.00	47.00	46.70
T2 (μs)	40.10	19.80	33.40	17.50	13.50
Gate error (10^{-3})	0.86	0.94	1.03	2.15	3.26
Readout error (10^{-2})	6.40	6.90	2.90	4.80	10.90
MultiQubit gate error (10^{-2})		**CX1_0** 2.74	**CX2_0** 2.16	**CX3_2** 7.96	**CX4_2** 7.33
			CX2_1 2.75	**CX3_4** 5.69	

IBM Q 5 Yorktown [ibmqx2]

ACTIVE: CALIBRATING

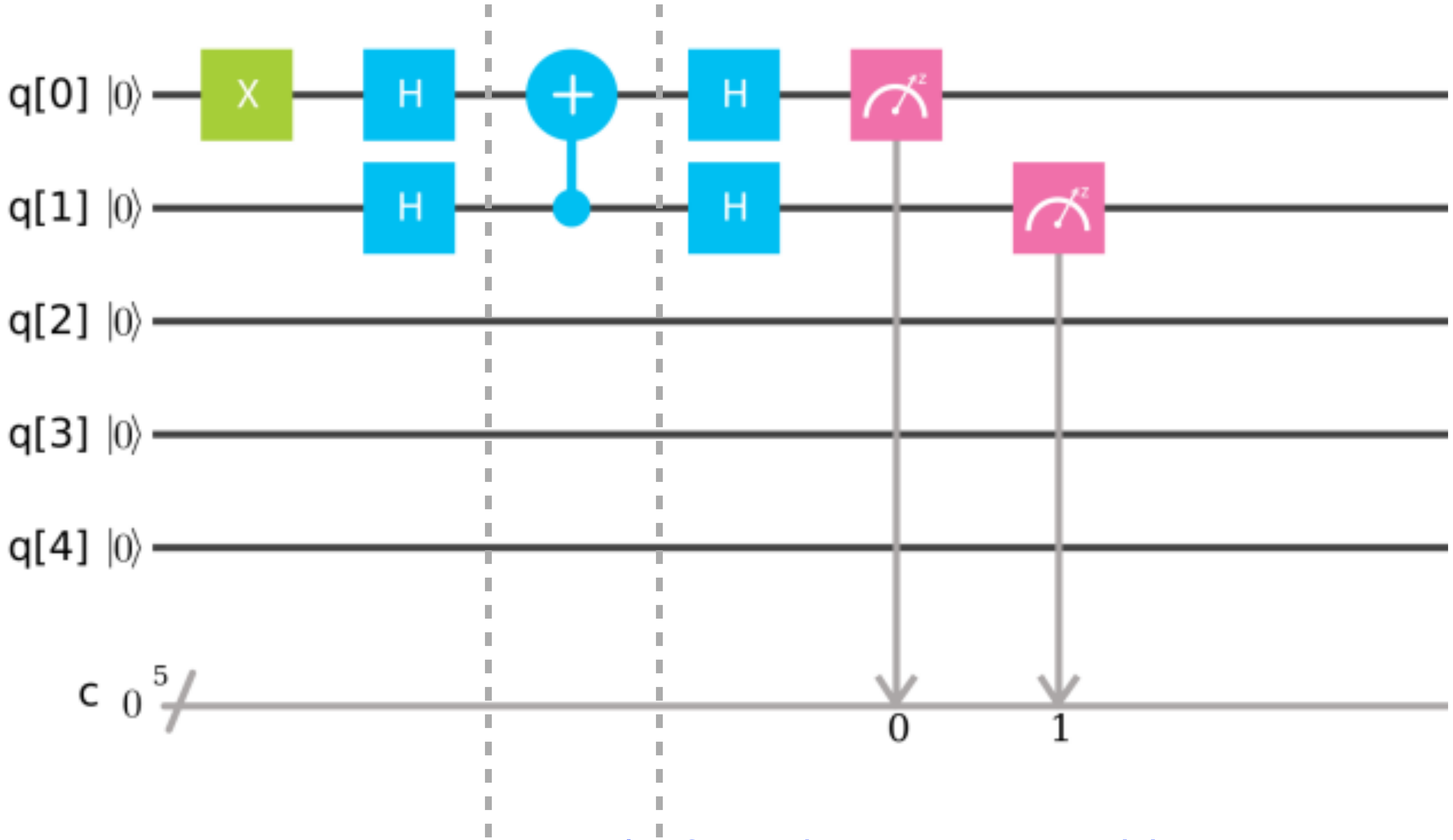
Deutsch-Jozsa: Quantum Computation "Hello World"

- Let us have ***f*: {0, 1}**^{N} **→ {0, 1}** that is promised to be either constant or balanced (nothing else). Balanced means the function vector has *exactly* $\mathbf{2^{N-1}}$ ones (and zeros).
  - we have to decide what kind of function we have
  - to give a deterministic answer classically, we need at least $\mathbf{2^{N-1} + 1}$ invocations of *f*
  - on a quantum computer, it suffices to do just one invocation of *f*
  - exponential speed up thanks to the quantum parallelism and interference

Simple Case for $N = 1$

$x, f(x)$	Constant function		Balanced function	
0	0	1	0	1
1	0	1	1	0

DJ Quantum Computation Scheme (with balanced f example)

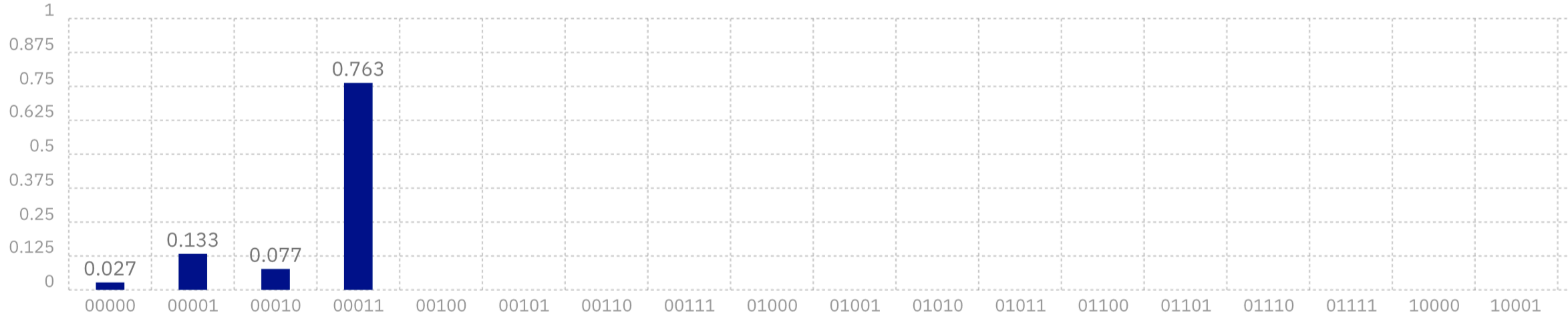


oracle function operator U_f

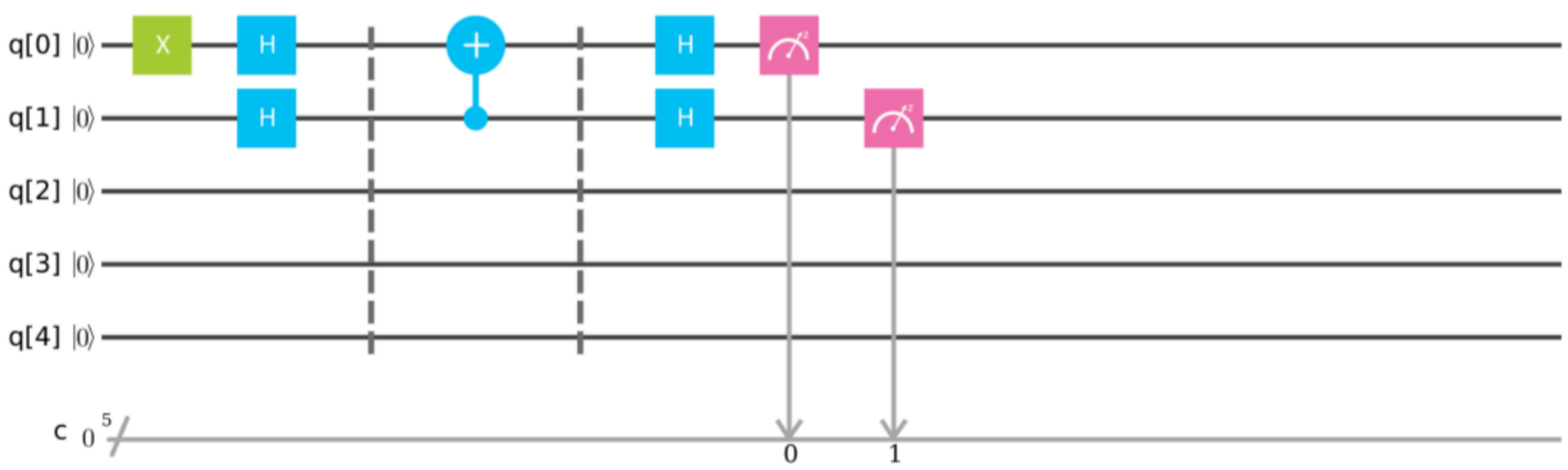
Device: ibmqx4

Quantum State: Computation Basis

Download CSV



Quantum Circuit



OPENQASM 2.0

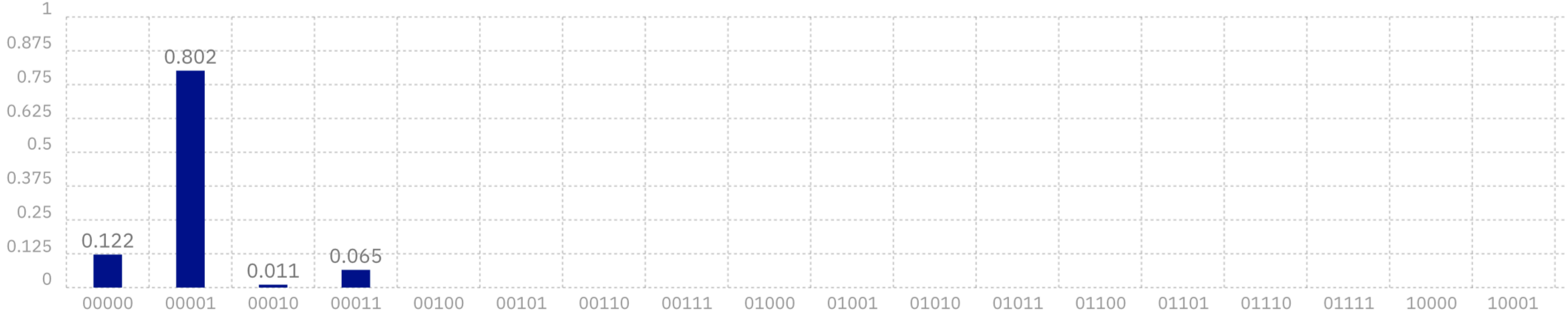
```
include "qelib1.inc";
qreg q[5];
creg c[5];

x q[0];
h q[0];
h q[1];

```

Open in Composer

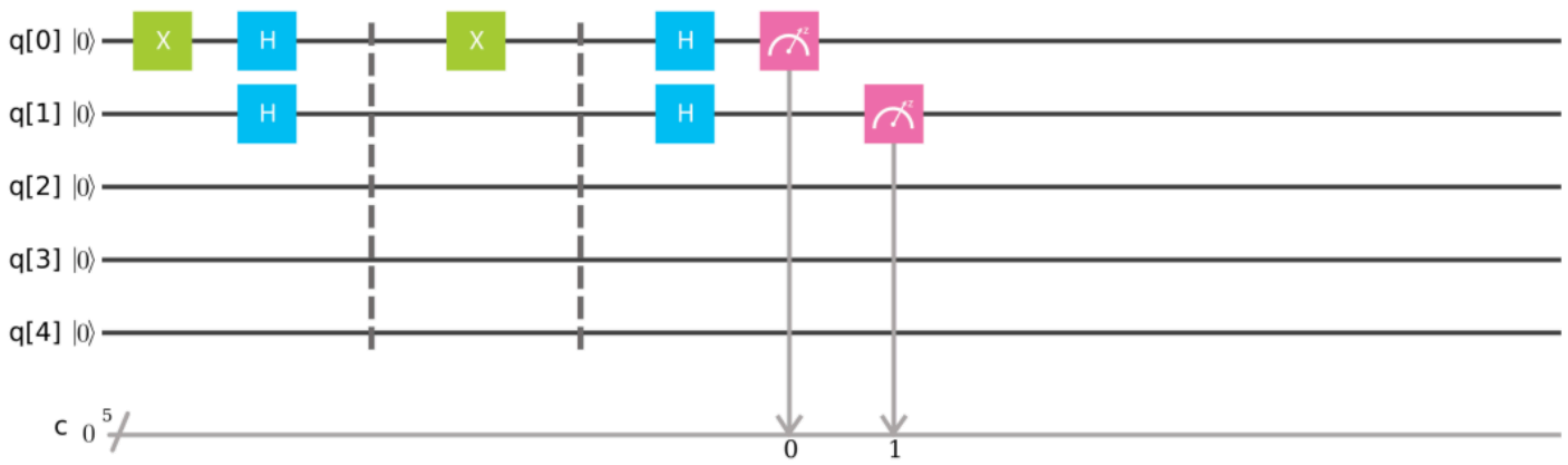
Device: ibmqx4

Quantum State: Computation Basis

Download CSV



Quantum Circuit



OPENQASM 2.0

```
include "qelib1.inc";
qreg q[5];
creg c[5];

x q[0];
h q[0];
h q[1];

```

Open in Composer

Earth Air Fire Water

RSA (since 1977)

easy way

$$x = y^e \bmod N$$

hard way

$$x, y < N$$

RSA - Going Back and Forth

$$x^d \bmod N = y$$

~~hard~~ easy way

$$x, y < N$$

How to get the private exponent “d”?

$$N = pq$$

$$d = e^{-1} \bmod lcm(p-1, q-1)$$

easy way if we can factorise *N*

Period Finding and Factorisation (Shor's Algorithm)

$$\text{Let } f(k) = a^k \bmod N$$

$$\text{and let us find } r: f(k+r) = f(k)$$

$$\Rightarrow a^{k+r} \bmod N = a^k \bmod N$$

$$\Rightarrow a^r \bmod N = 1, \text{so } N \text{ divides } a^r - 1$$

$$\Rightarrow \text{for even } r,\ N \text{ divides } (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$$

$$\Rightarrow \text{for } N \nmid (a^{\frac{r}{2}} \pm 1),\ \gcd(a^{\frac{r}{2}} \pm 1, N) \text{ are factors of } N$$

Quantum Parallelism…

$$|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle |a^k \bmod N\rangle$$

Quantum Parallelism… (Example)

$$|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle |a^k \bmod N\rangle$$

$$M = 16, N = 15, a = 7$$

$$|\psi\rangle = \frac{1}{4}\left(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + \ldots + |15\rangle|13\rangle\right)$$

Feeling of the Period

$$\begin{aligned}|\psi\rangle = &\frac{1}{4}\big(|0\rangle+|4\rangle+|8\rangle+|12\rangle\big)|1\rangle\\ &+\frac{1}{4}\big(|1\rangle+|5\rangle+|9\rangle+|13\rangle\big)|7\rangle\\ &+\frac{1}{4}\big(|2\rangle+|6\rangle+|10\rangle+|14\rangle\big)|4\rangle\\ &+\frac{1}{4}\big(|3\rangle+|7\rangle+|11\rangle+|15\rangle\big)|13\rangle\end{aligned}$$

Quantum Fourier Transform (QFT) of Eigenstate

$$\left|ur+k\right\rangle\left|a^k\right\rangle \to \frac{1}{\sqrt{m}}\sum_{v=0}^{m-1} e^{\frac{2\pi i(ur+k)v}{m}}\left|v\right\rangle\left|a^k\right\rangle$$

$$= \frac{1}{\sqrt{m}}\left(\sum_{v=0}^{m-1} \underbrace{e^{\frac{2\pi ikv}{m}}}_{\text{fixed phase swallow}} \cdot \underbrace{e^{\frac{2\pi iuv}{\frac{m}{r}}}}_{\text{interference control}}\left|v\right\rangle\left|a^k\right\rangle\right)$$

fixed phase swallow   interference control

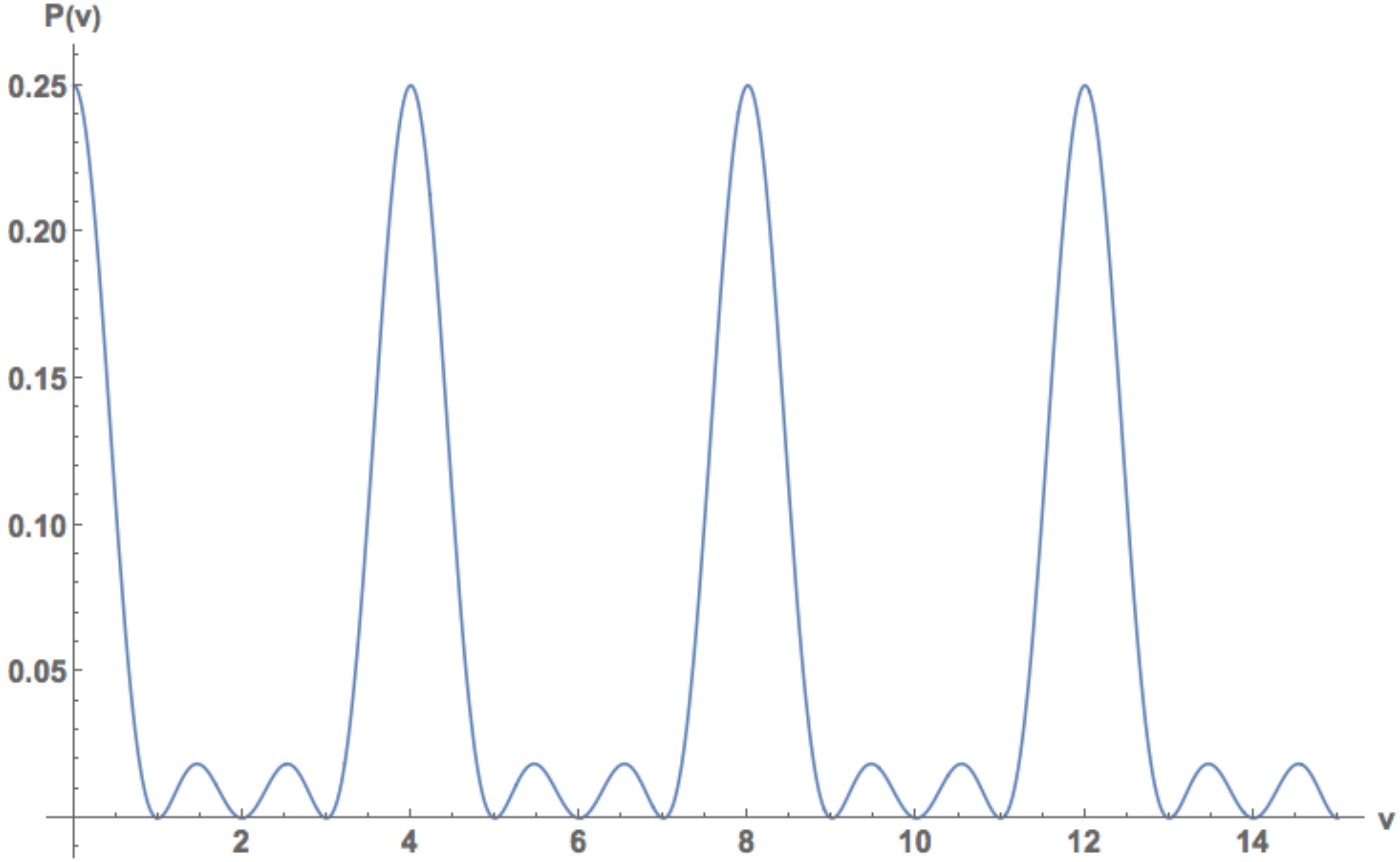
Superposing QFT

$$\sum_{(u)} \left|ur+k\right\rangle \left|a^k\right\rangle \to \frac{1}{\sqrt{m}} \sum_{(u)} \sum_{v=0}^{m-1} e^{\frac{2\pi i(ur+k)v}{m}} \left|v\right\rangle \left|a^k\right\rangle$$

$$= \frac{1}{\sqrt{m}} \left[\sum_{v=0}^{m-1} \underbrace{e^{\frac{2\pi ikv}{m}}}_{\text{fixed phase swallow}} \left(\sum_{(u)} \underbrace{e^{\frac{2\pi iuv}{\frac{m}{r}}}}_{\text{interference control}} \left|v\right\rangle \left|a^k\right\rangle \right) \right]$$

fixed phase swallow   interference control

Exploiting the Parallelism via QFT Interference



It is not only about the Shor's algorithm

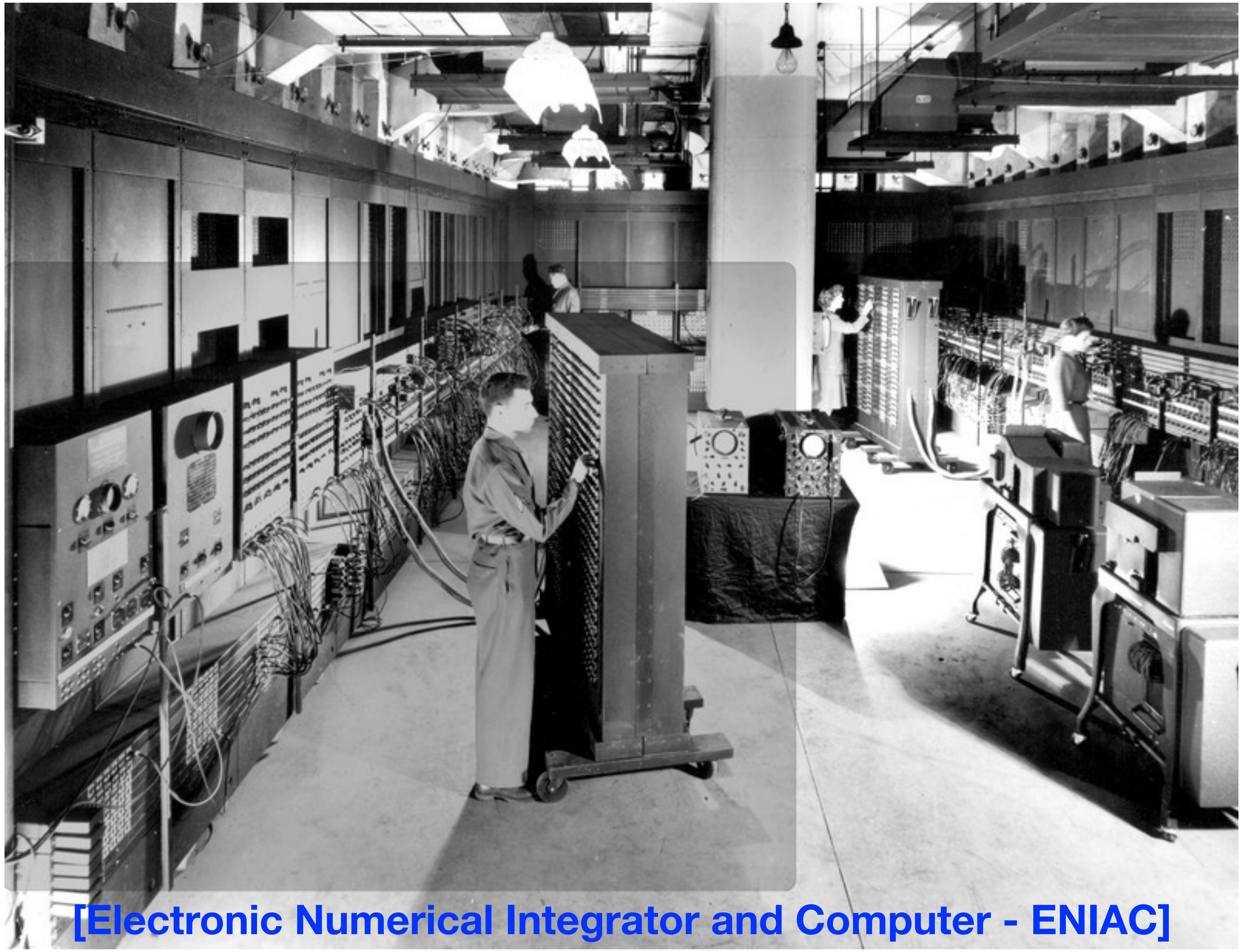
- **Grover's search method**
  - quadratic speed-up, usable for both asymmetric and symmetric algorithms
- **Simon's period finding**
  - exponencial speed-up, usable for both asymmetric and symmetric algorithms
- **Hidden subgroup problem**
  - exponencial speed-up
  - generalises Simon's, Shor's, and a lot of other algorithms

— http://quantumalgorithmzoo.org


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 © 2012 Scott Adams, Inc. /Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

Main Challenges for Quantum Computers Today

- We have a **Noisy Intermediate-Scale Quantum** (NISQ) technology
  - coherence time
  - scalability



[Electronic Numerical Integrator and Computer - ENIAC]

IBM Q quantum computing systems

Microwave electronics

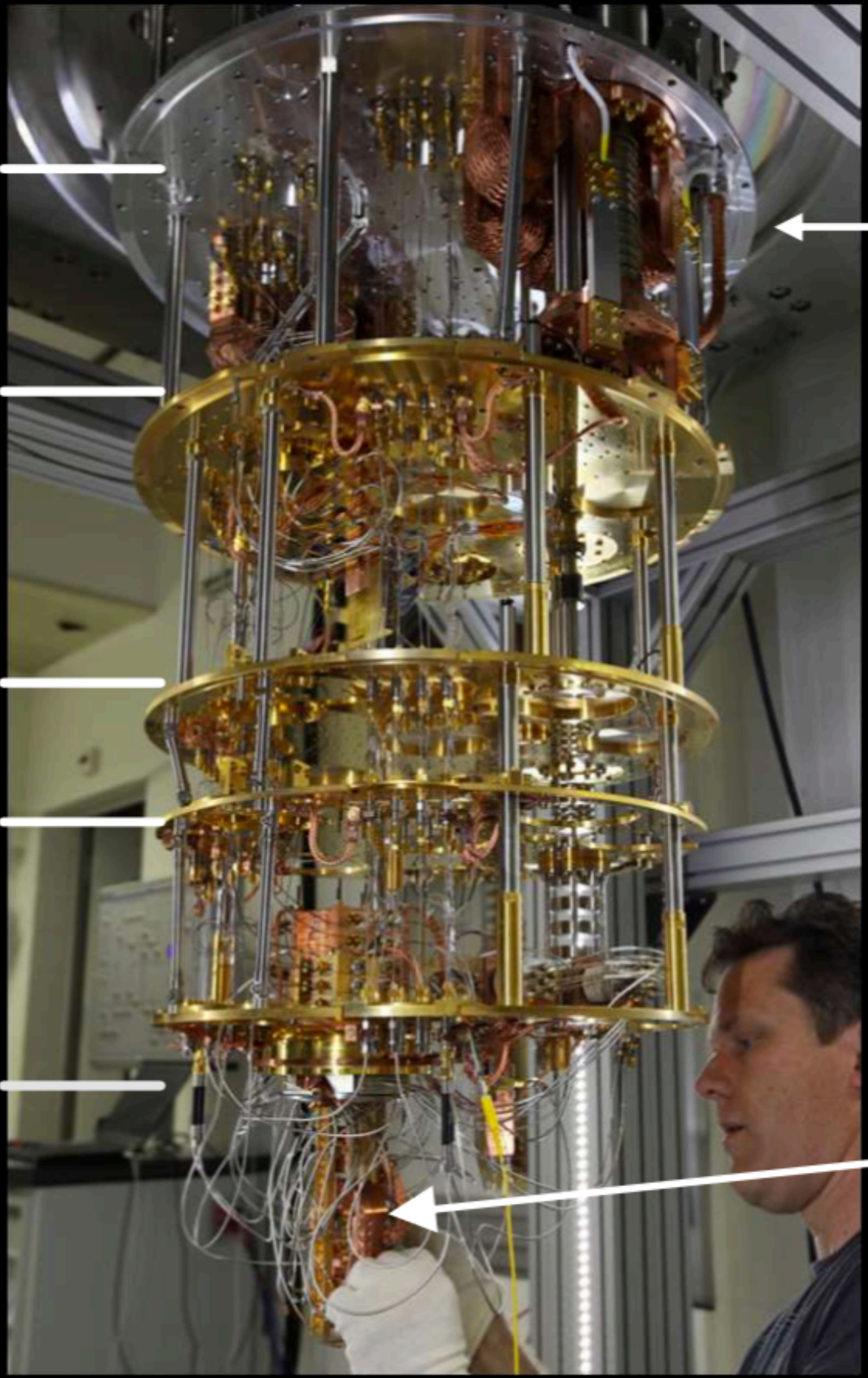
40K

3K

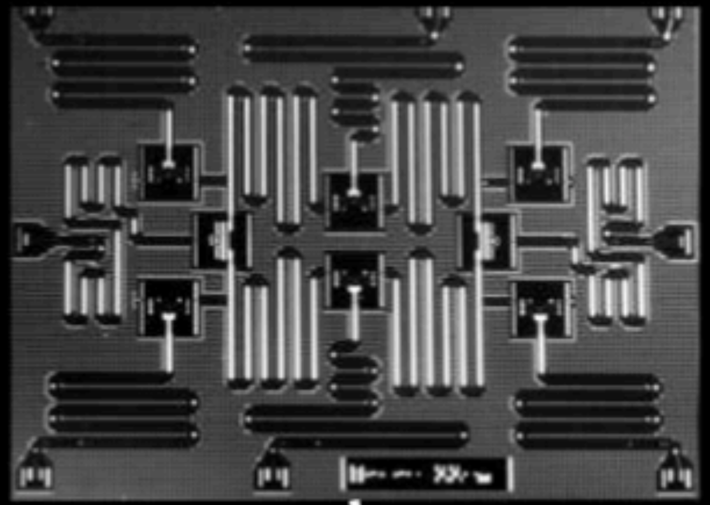
0.9K

0.1K

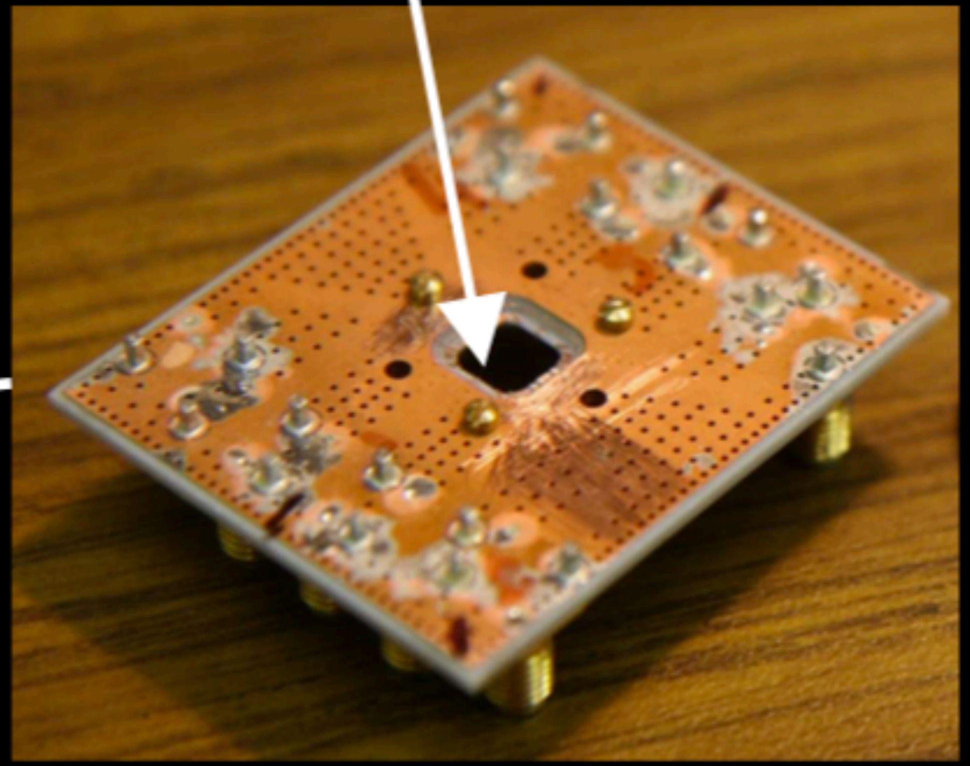
0.015K



Refrigerator to cool qubits to 10 - 15 mK with a mixture of ^{3}He and ^{4}He



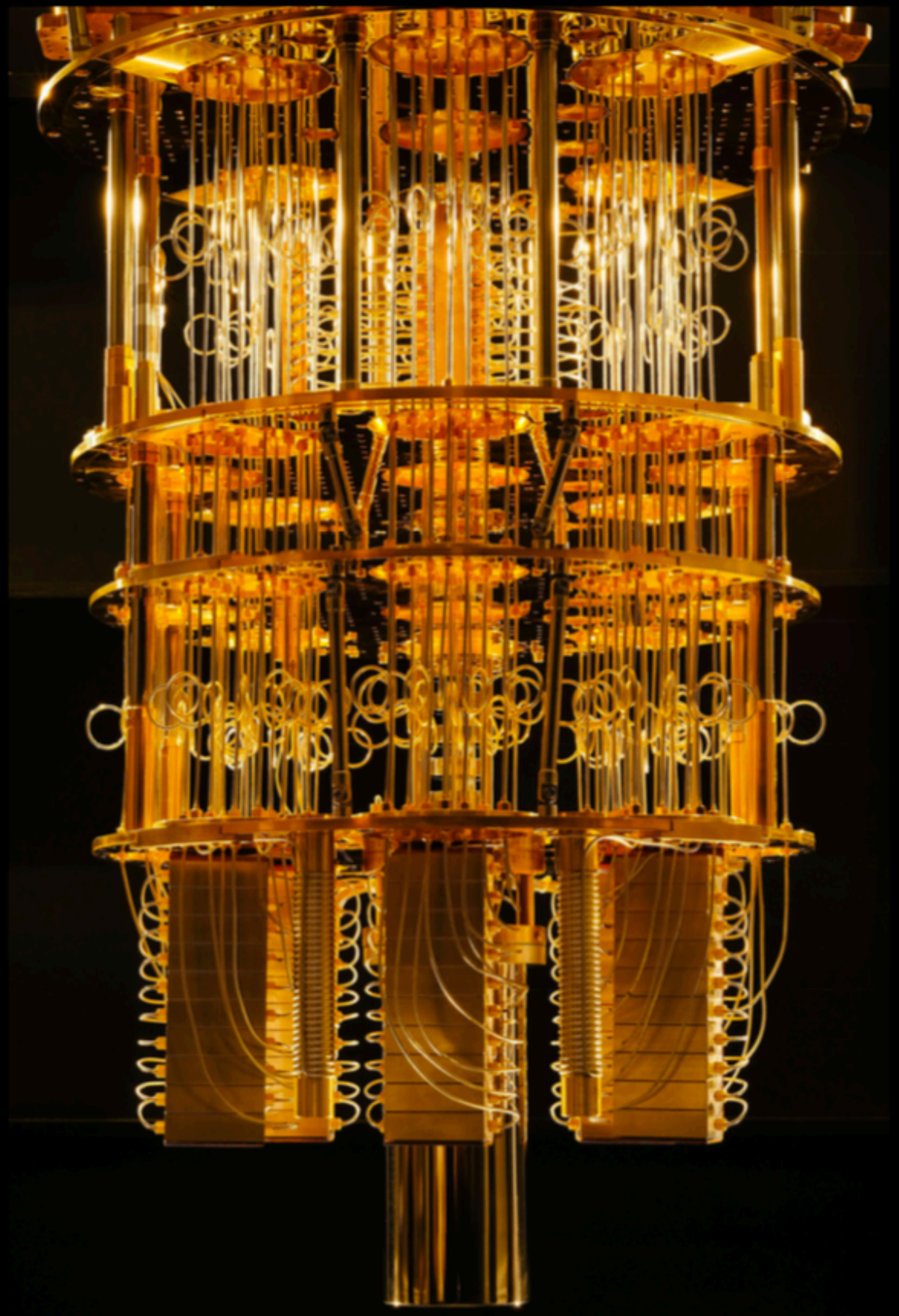
Chip with superconducting qubits and resonators



PCB with the qubit chip at 15 mK
Protected from the environment by multiple shields

[Sutor, 2018]

How many qubits are required to see quantum improvement?



Estimate of the number of “good” qubits required before quantum computing shows advantage over conventional:

Problem	Type of Quantum Computer	# Qubits for advantage (est)	Years to advantage (est)
Quantum Chemistry	NISQ/Approximate QC	$10^2 \sim 10^3$	< 5 ?
Optimization (specific)	NISQ/Approximate QC	$10^2 \sim 10^3$	< 5 ?
Heuristic machine learning	NISQ/Approximate QC	$10^2 \sim 10^3$	< 5 ?
Shor’s algorithm	Universal fault-tolerant QC	$> 10^8$	> 10~15 **if possible**
Big Linear Algebra Programs (FEM)	Universal fault-tolerant QC	$> 10^8$	> 10~15 **if possible**

[Sutor, 2018]

“Quantum Computing: Progress and Prospects”

Key Finding 1: *Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm- based public key cryptosystems will be built within the next decade.*

— http://nap.edu/25196

"Quantum Computing: Progress and Prospects"

Key Finding 10: *Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of* ***post-quantum cryptography*** *is critical for minimizing the chance of a potential security and privacy disaster.*

— http://nap.edu/25196

Conclusions

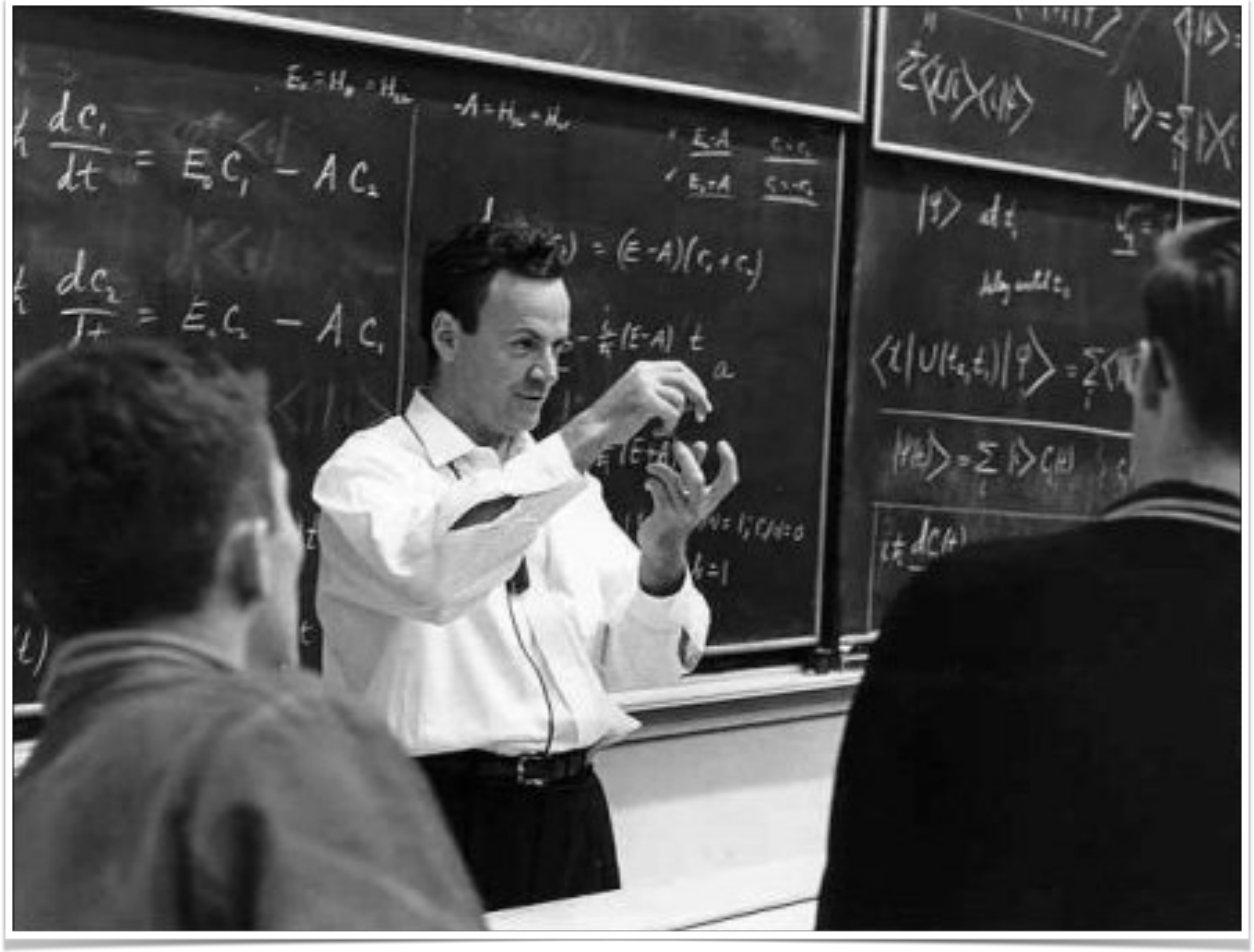
- Quantum computers are not an immediate threat, they are rather a big opportunity for other areas, such as e.g. chemistry, optimisation tasks, and financial mathematics, now

- However, they are mid / long-term threat, so **be careful about retroactive cryptanalysis**

- Follow upcoming recommendation of cryptologists

- Be careful when implementing symmetric encryption on quantum hardware

- When appropriate, migrate to a quantum resistant public key cryptosystem



Physics is like sex: sure, it may give some practical results, but that's not why we do it.

Richard Phillips Feynman
(1918 - 1988, Nobel Prize in Physics 1965)