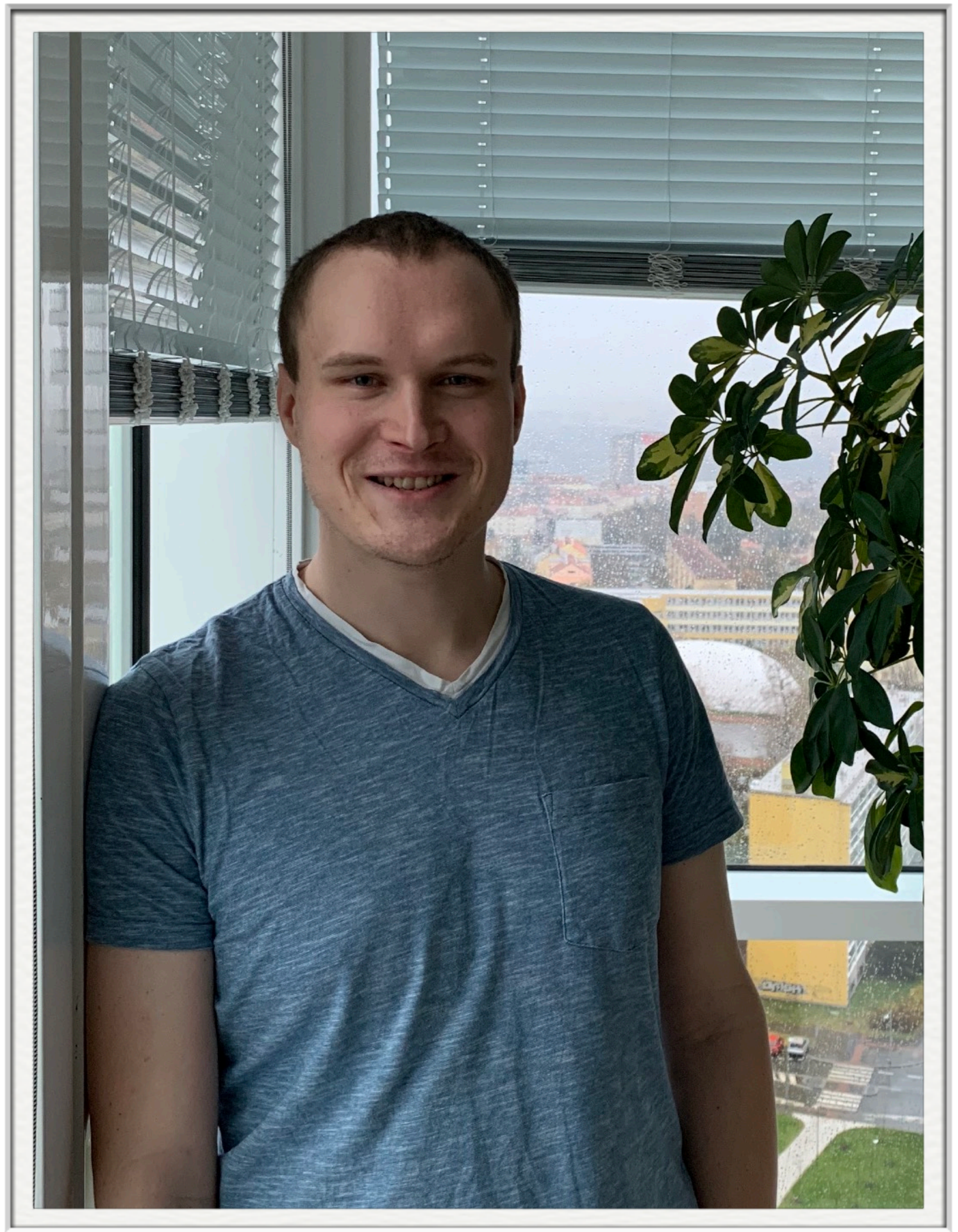
Quantum Computation Fundamentals

Tomáš Rosa, Ph.D.
Cryptology and Biometrics Competence Centre and Quantum Computations Innovation Lab
Raiffeisen BANK International

Cryptology and Biometrics Competence Centre

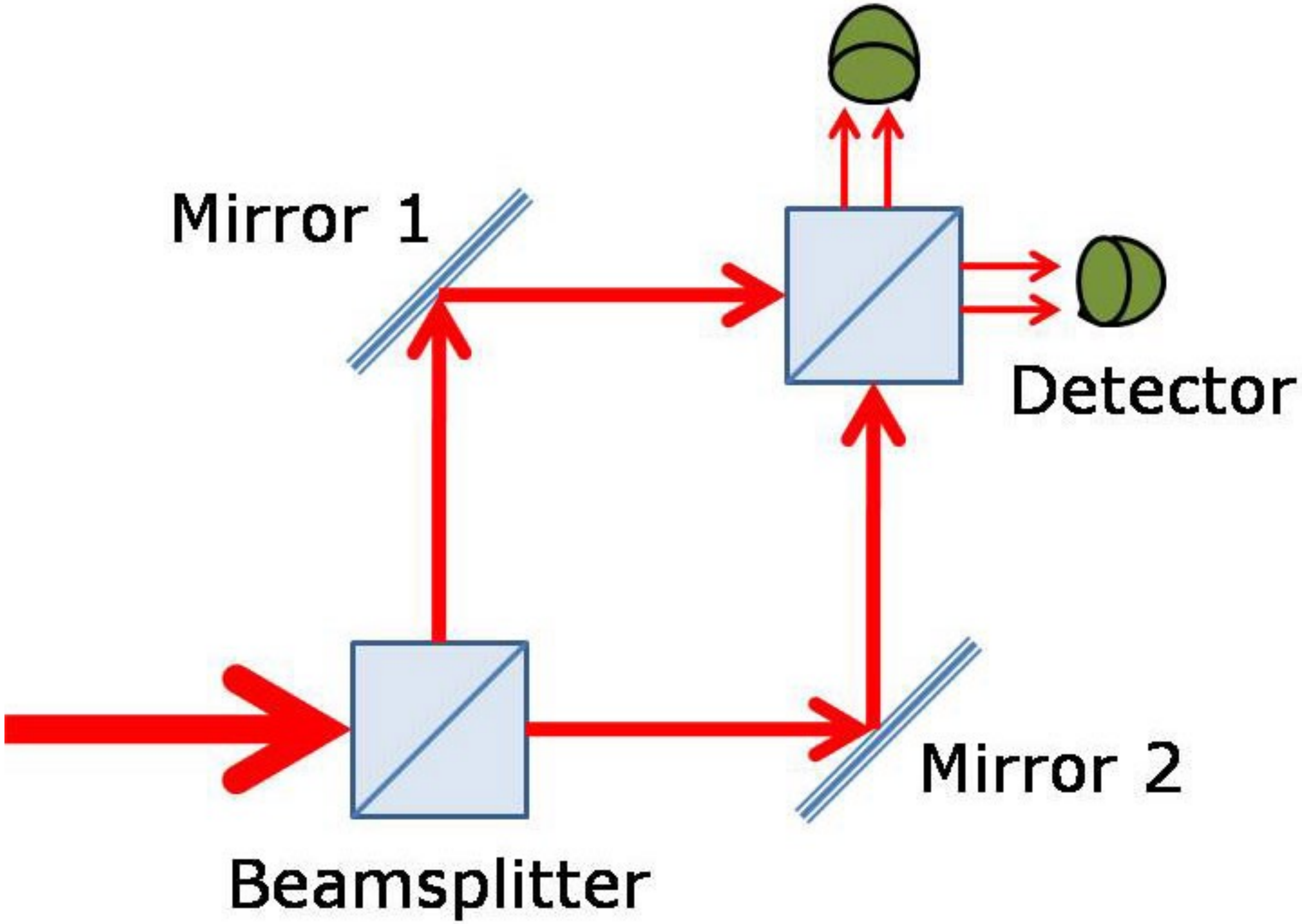


Jiří Pavlů
Ph.D. candidate in cryptology
jiri.pavlu@rb.cz

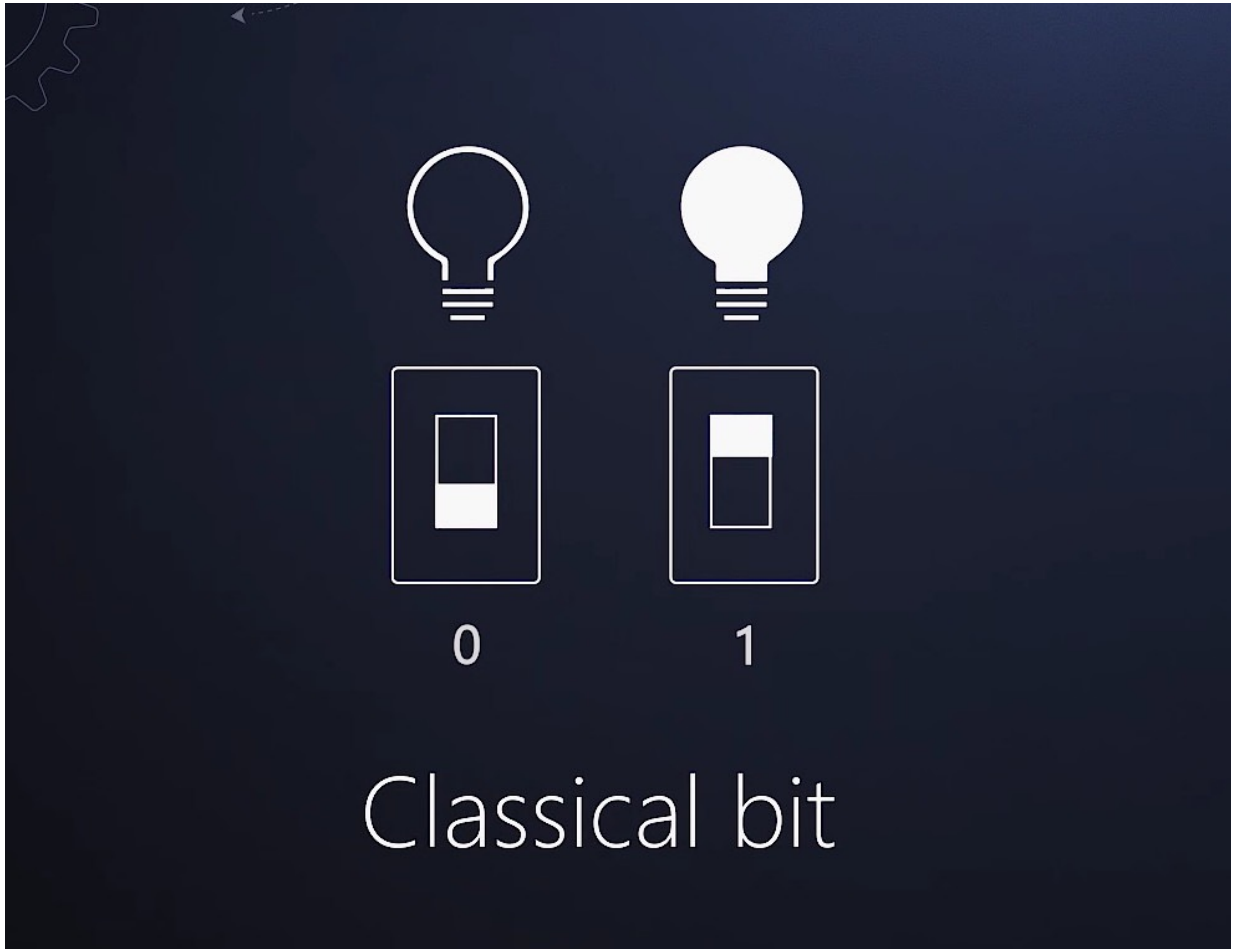
crypto@rb.cz

Tomáš Rosa
Ph.D. in cryptology
tomas.rosa@rb.cz

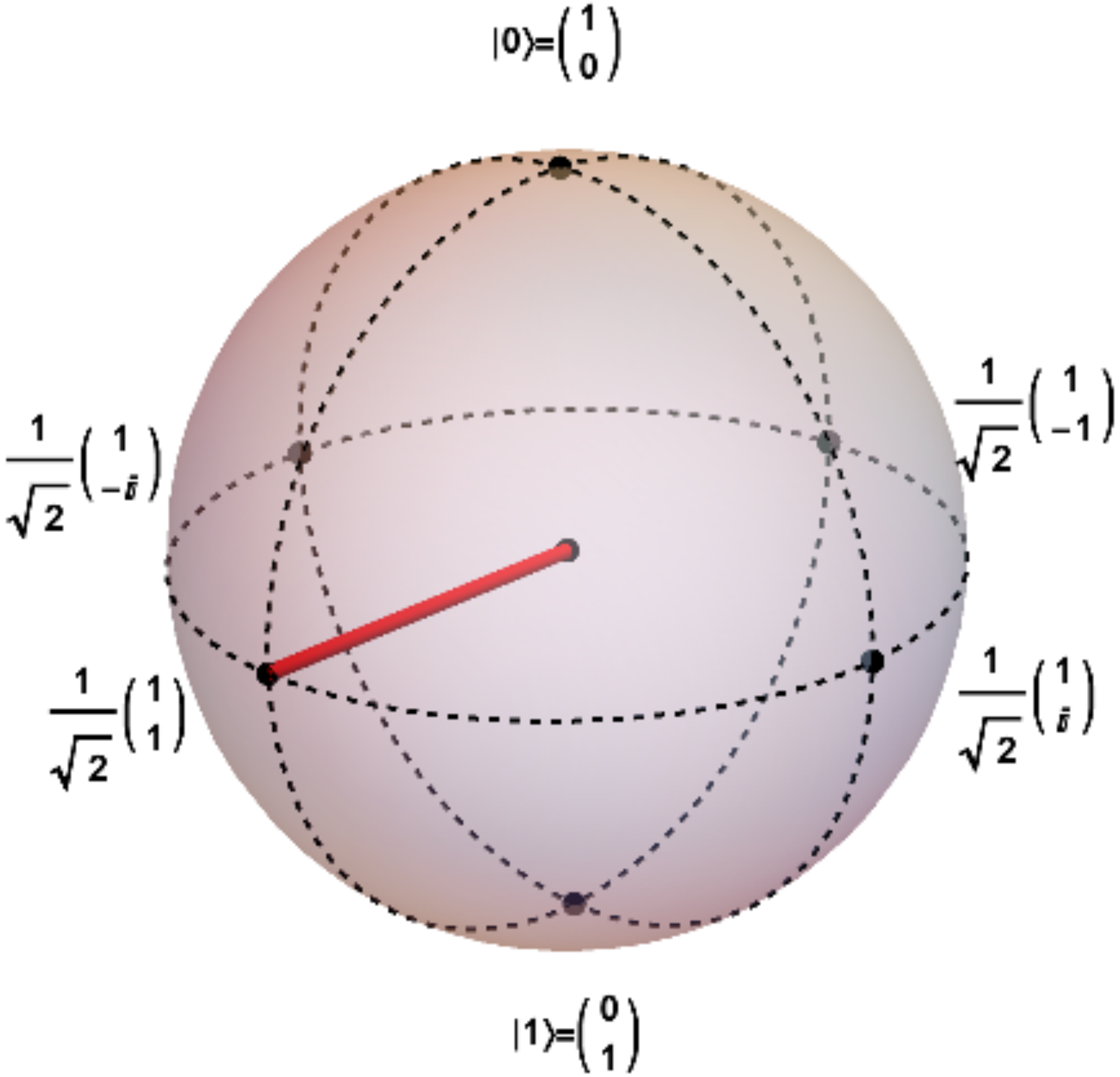
Mach-Zehnder Experiment Tells ***a Lot*** of the Story



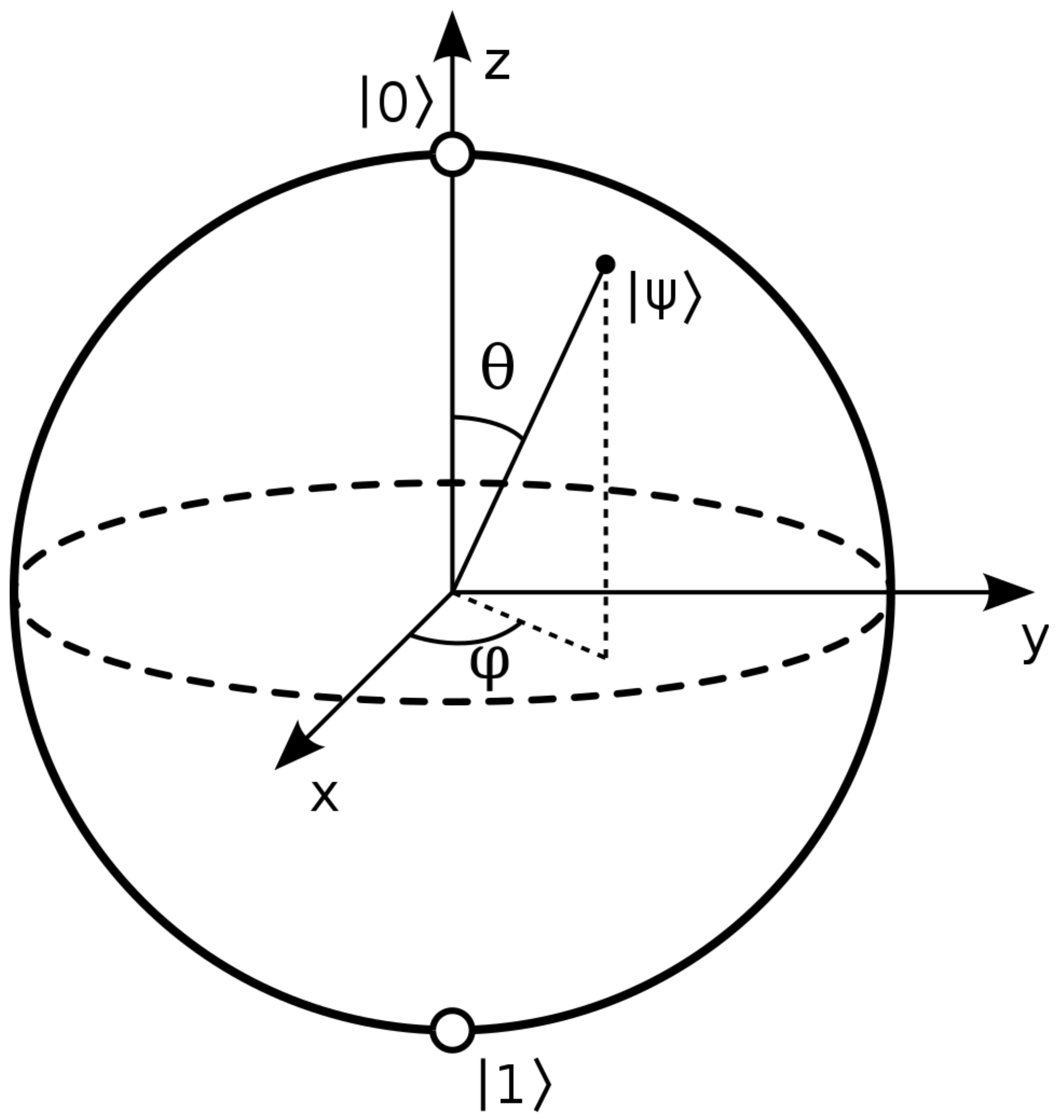
Classical Computer - Classical Bit



Quantum Computer - Quantum Bit (Qubit)



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



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

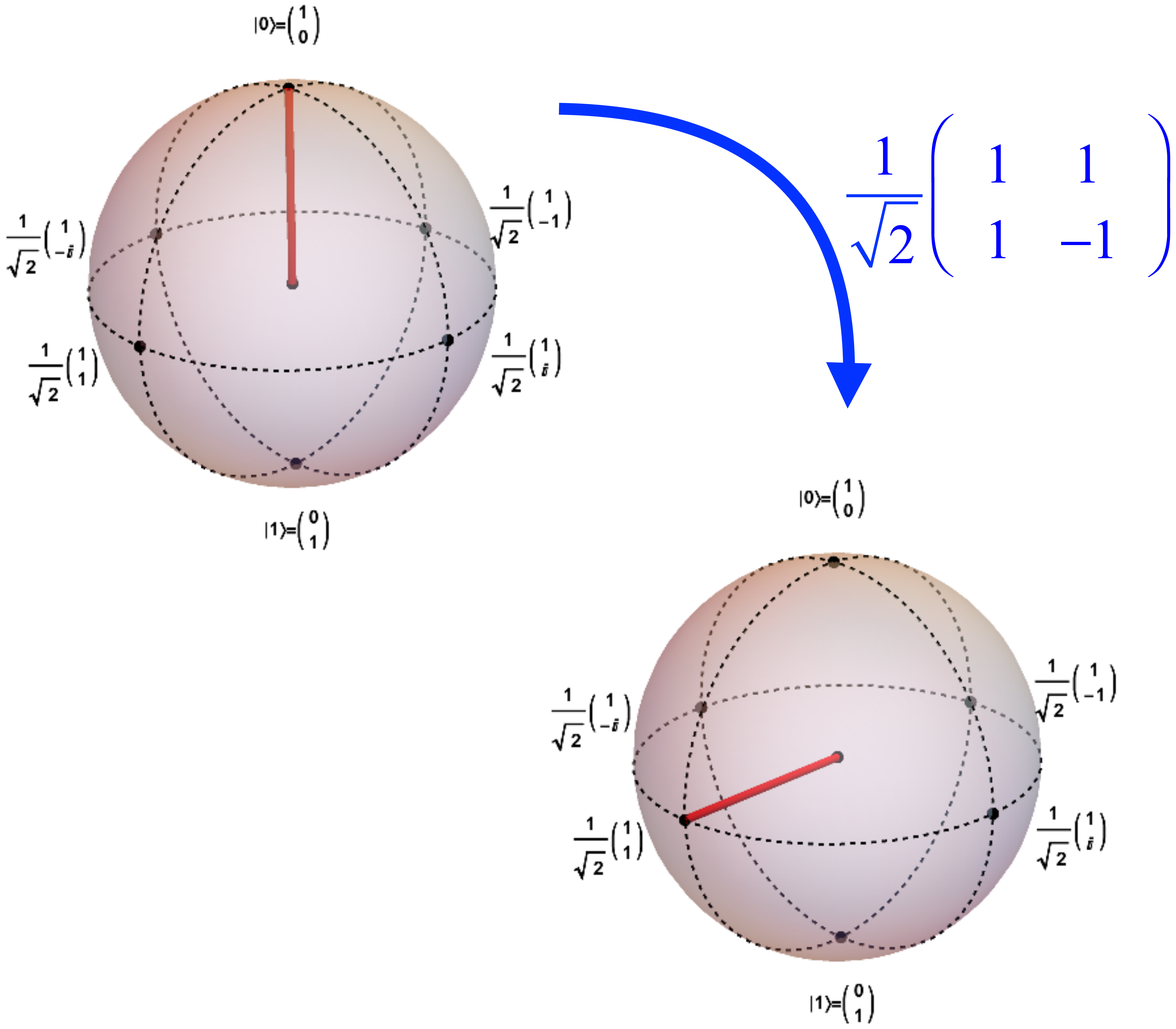
$$|\omega_0|^2 + |\omega_1|^2 = 1$$

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

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

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

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



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

Postulate #3: Projective probabilistic measurement

- When measured, quantum state collapses into one of particular eigenstates comprising the basis vectors of the corresponding Hilbert space.

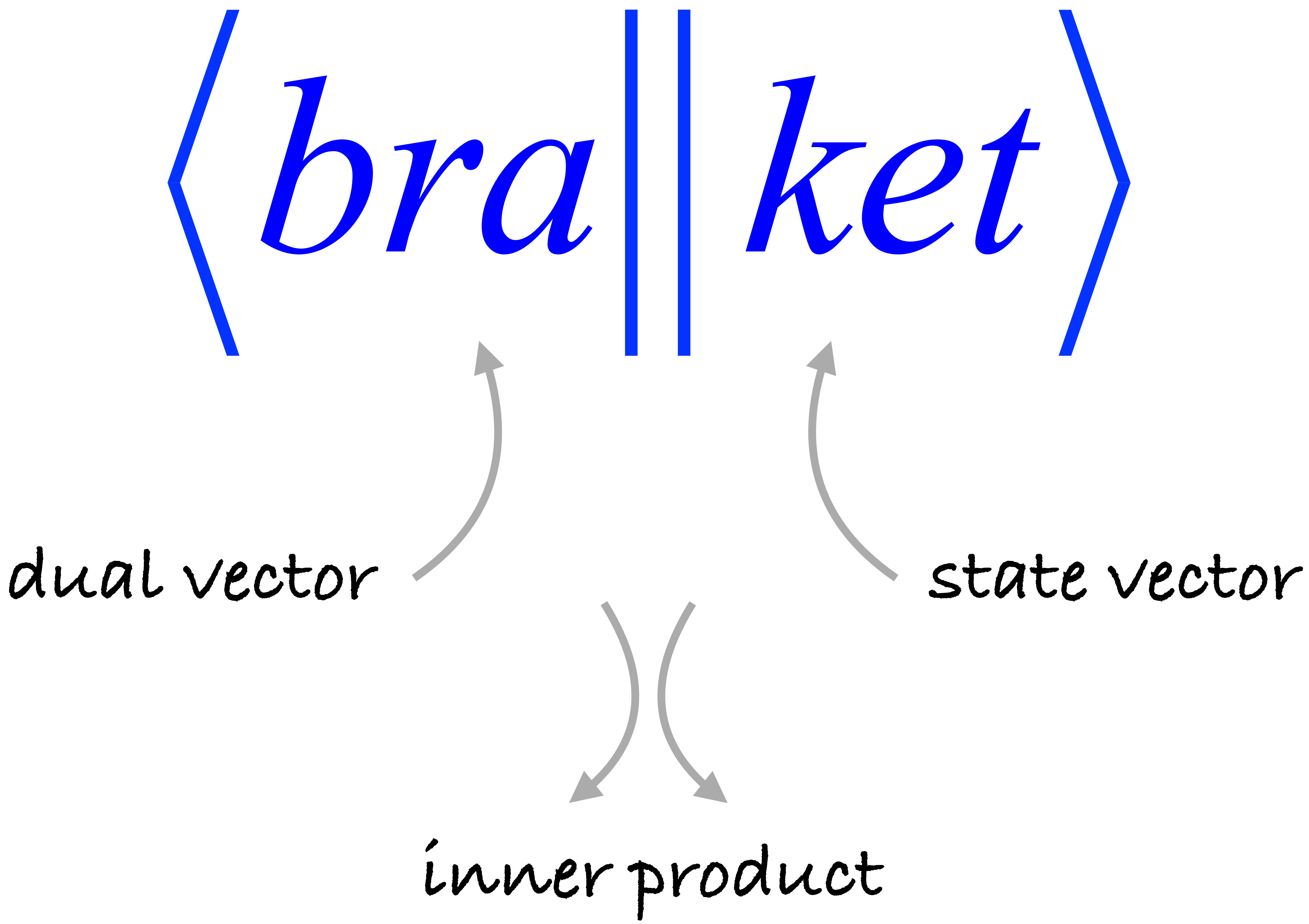
- For a qubit, these are labeled **|0>** and **|1>**. So called computational basis.

- Superposition cannot be seen directly. It governs the probability of the measurement outcome; coefficients ω_i called ***probability amplitudes***.

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

$$= \langle\psi||i\rangle\langle i||\psi\rangle$$

Dirac's Bra-Ket Notation



Dirac’s Bra-Ket Notation

$|ket\rangle$

$\langle bra|$

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.

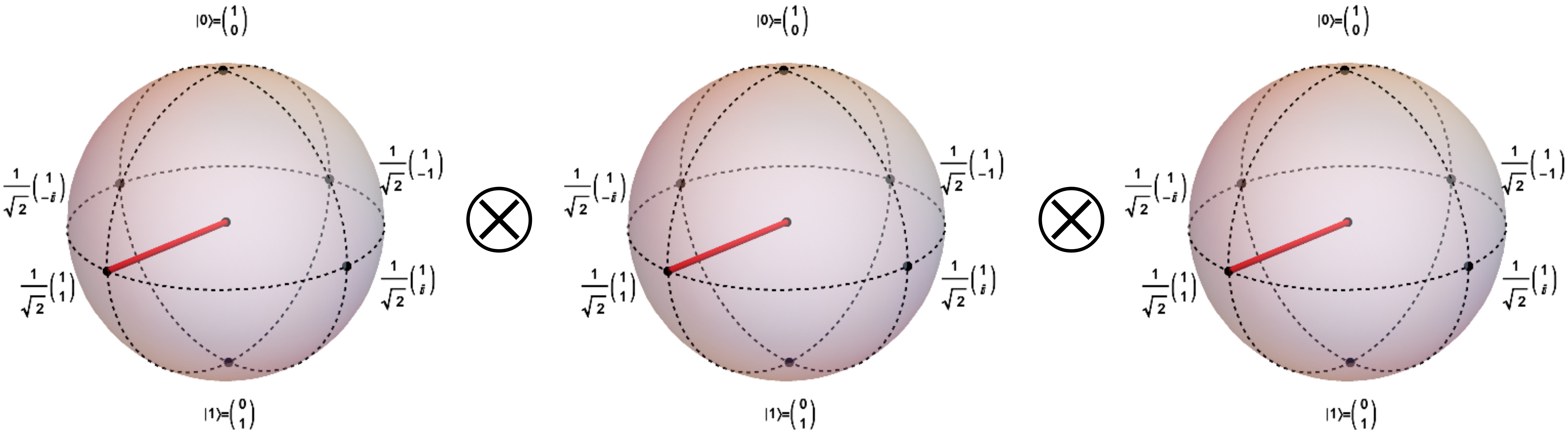
  - together with linear operators acting on this register, this is the source of so-called **quantum parallelism**

  - 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>**

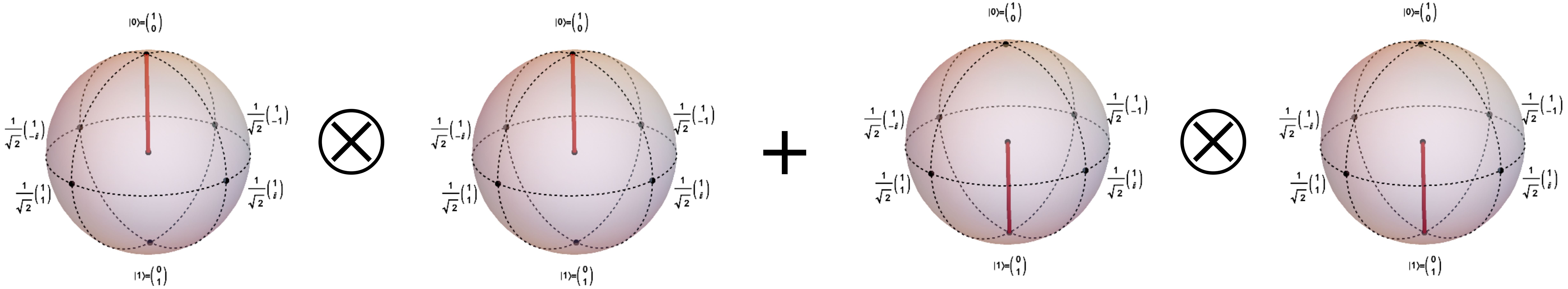
  - sometimes, the tensor product is noted explicitly |00…0> = |0>|0>…|0>, etc.

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



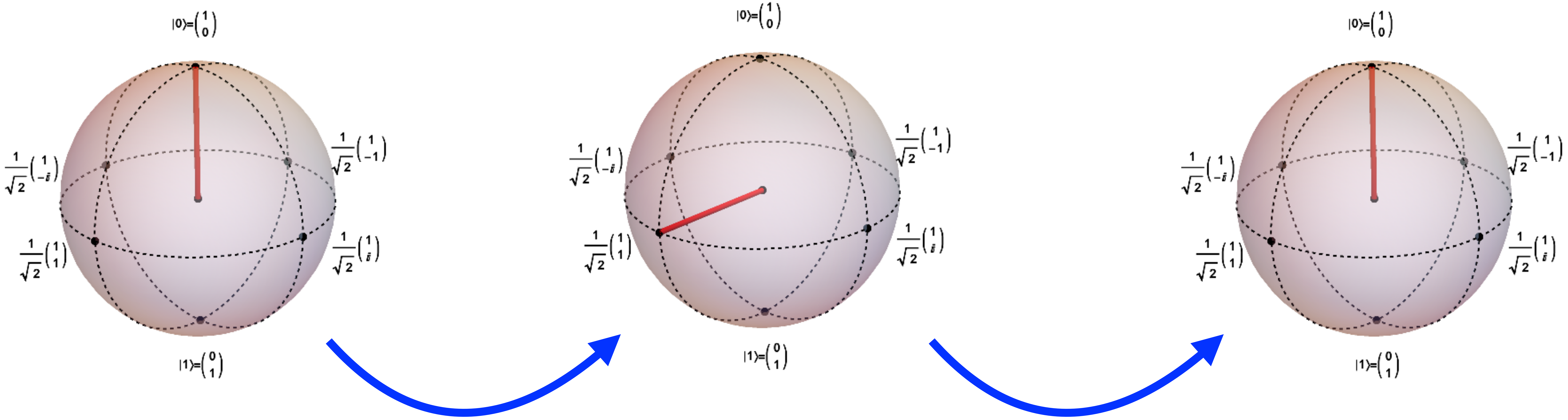
$$|\psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$

Entanglement (Note the Unavoidable Sum of Tensor Products…)



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

Quantum Operator/Instruction Flow Example ("Blinky" Experiment)



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

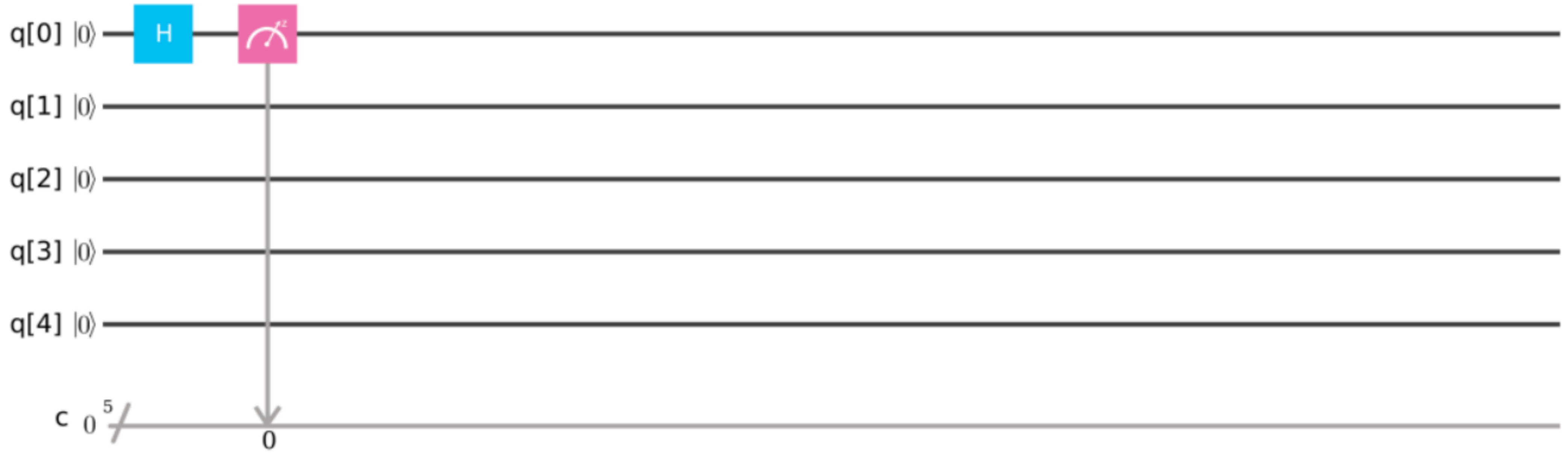
— *also showing the computational interference beyond the reach of classical probabilistic machines*
— *also resembling the Mach-Zehnder constructive/destructive interference experiment*

Quantum “Blinky” Project

Quantum State: Computation Basis

Download CSV

Quantum Circuit



OPENQASM 2.0

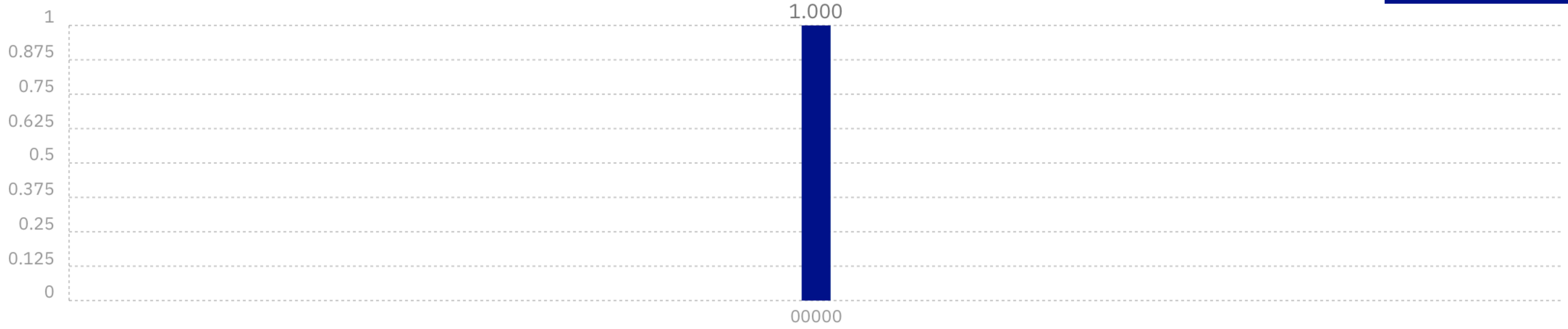
```
include "qelib1.inc";
qreg q[5];
creg c[5];

h q[0];

measure q[0] -> c[0];

```

Open in Composer

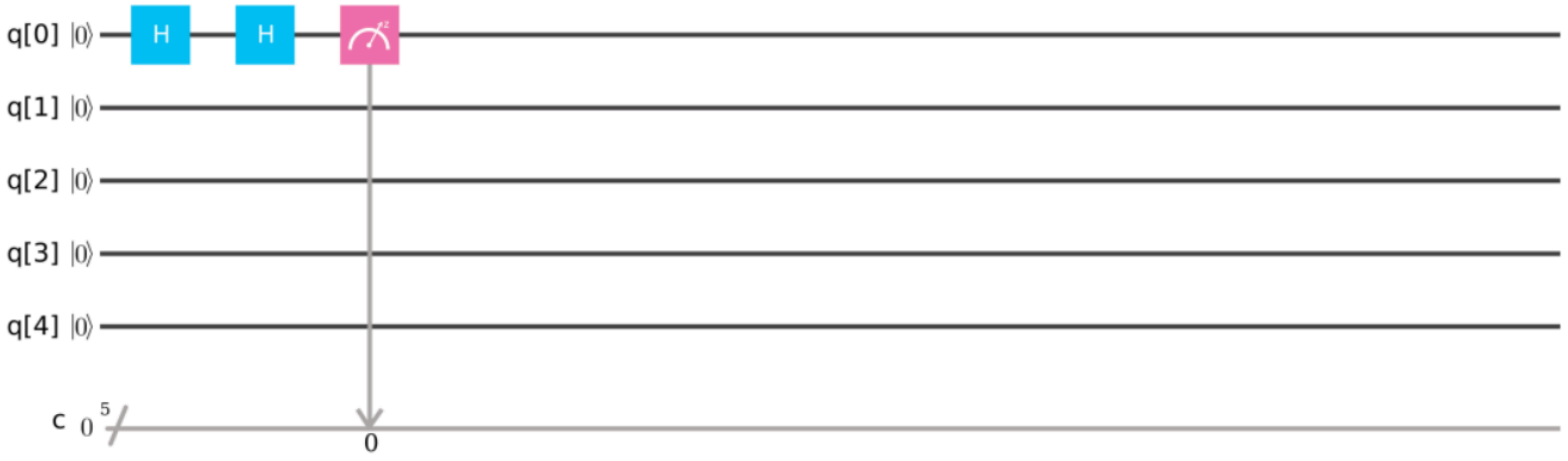
Edit in QASM Editor

Quantum State: Computation Basis

Download CSV



Quantum Circuit



OPENQASM 2.0

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

h q[0];
h q[0];

measure q[0] -> c[0];
```

Open in Composer

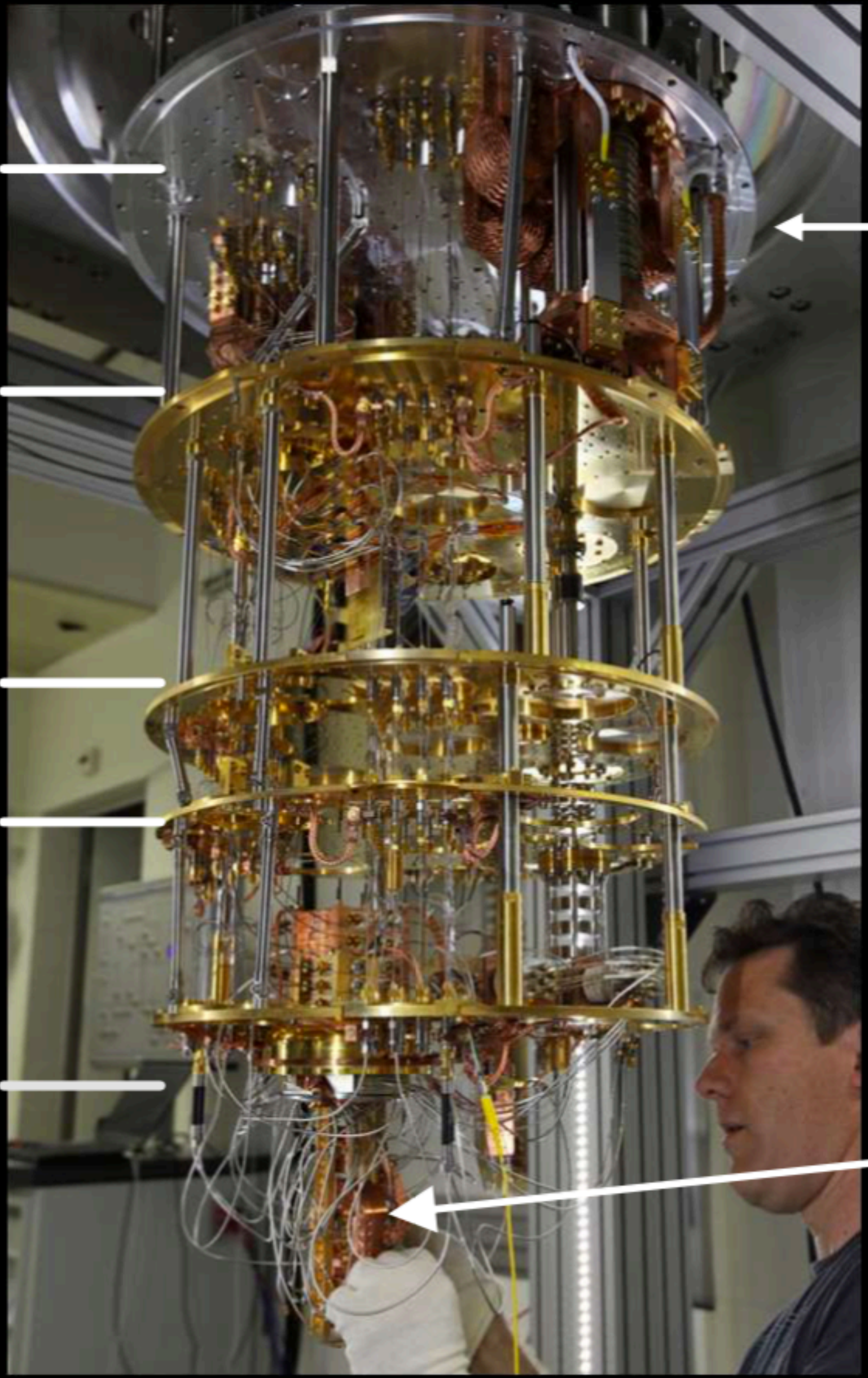
Edit in QASM Editor

Quantum Computational Paradigms (circuit-based model)

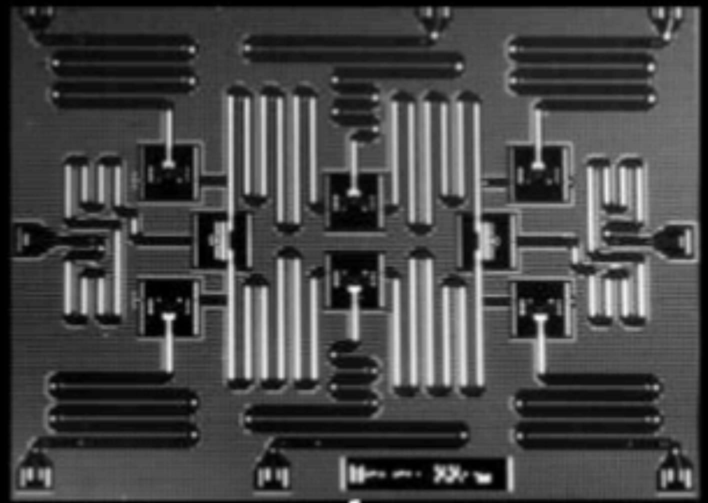
- quantum parallelism
  - since dimension grows exponentially and operators are linear
- interference, both constructive and destructive
  - enabled by the complex probability amplitudes
  - actually, we are working with complex probability “square” roots
- entangled states
  - delivering extra salt grain to the algorithms

IBM Q quantum computing systems

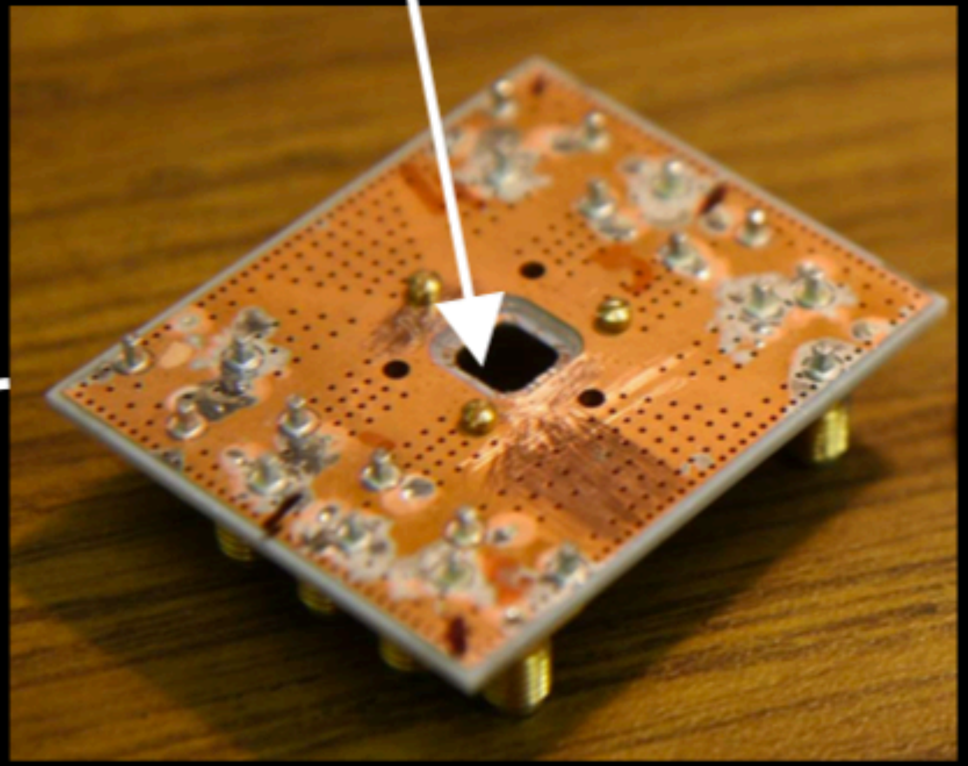
Microwave electronics



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



Chip with superconducting qubits and resonators

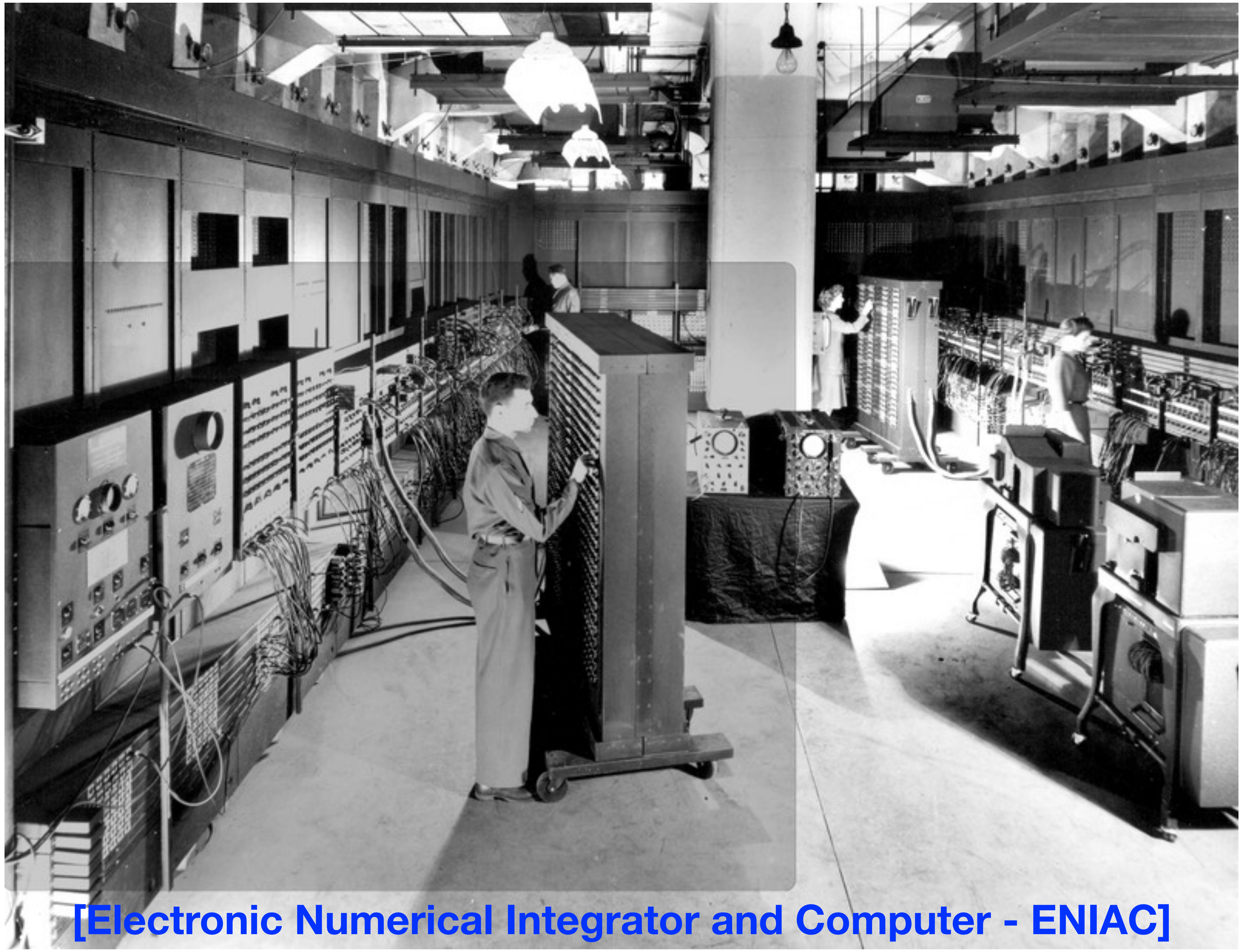


PCB with the qubit chip at 15 mK
Protected from the environment by multiple shields

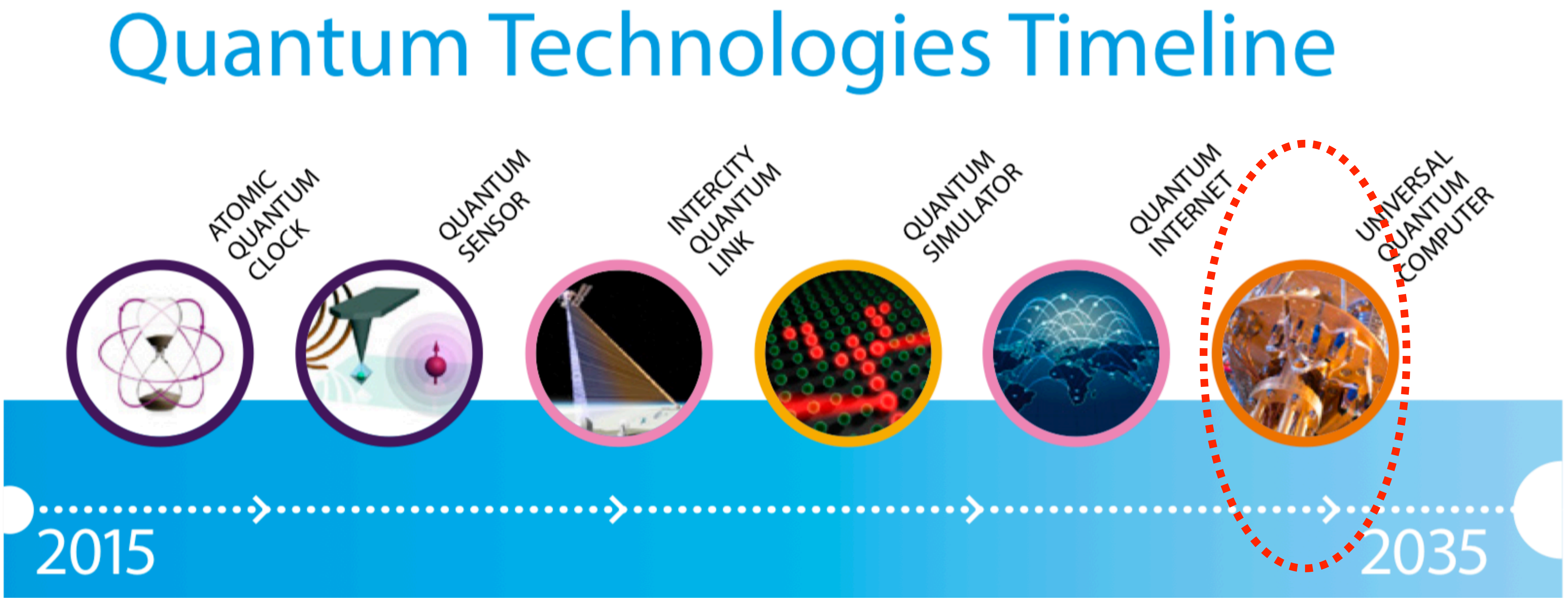
[Sutor, 2018]

Main Challenges for Quantum Computers Today

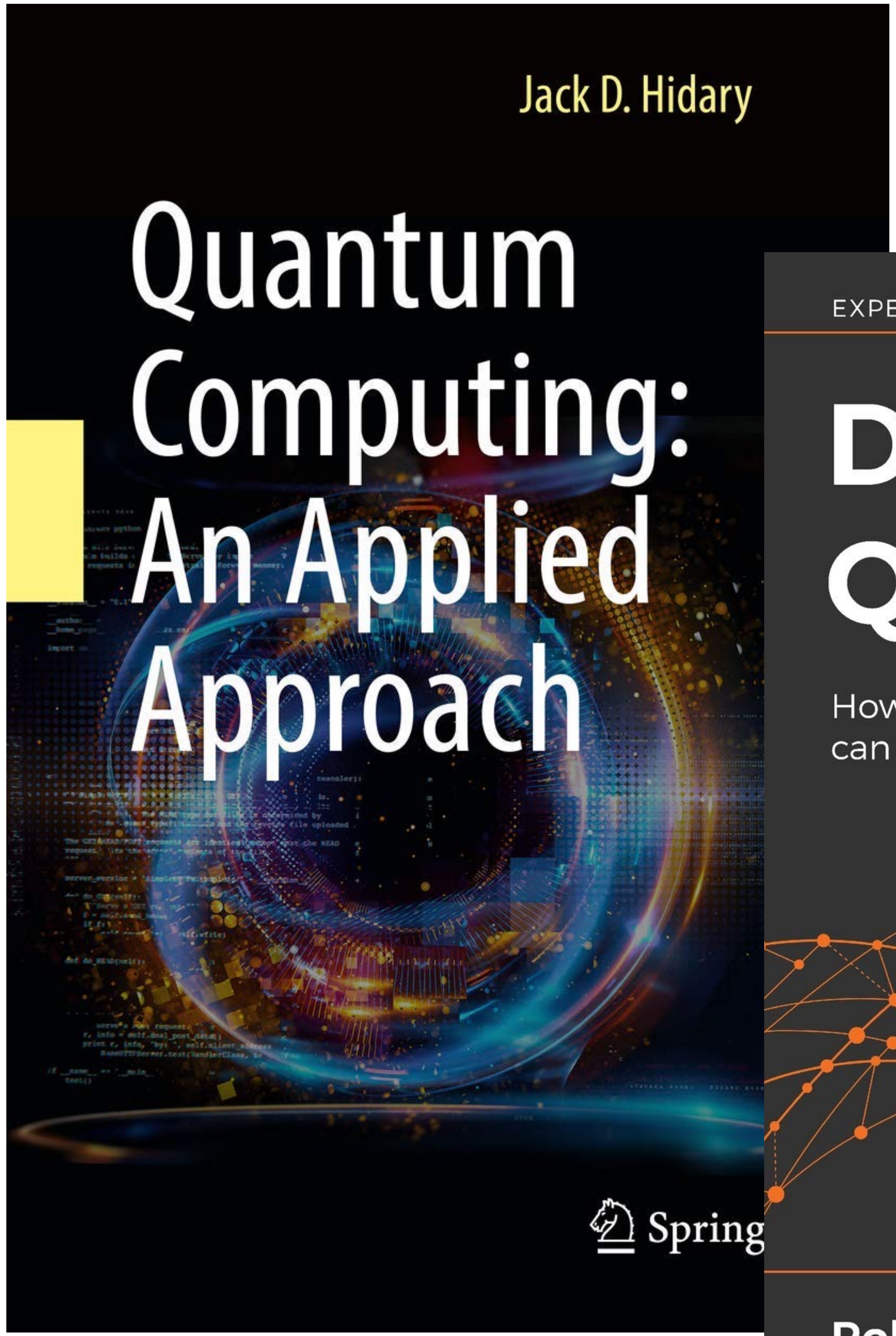
- We have a Noisy **Intermediate-Scale Quantum** (NISQ) technology
  - coherence time
  - scalability

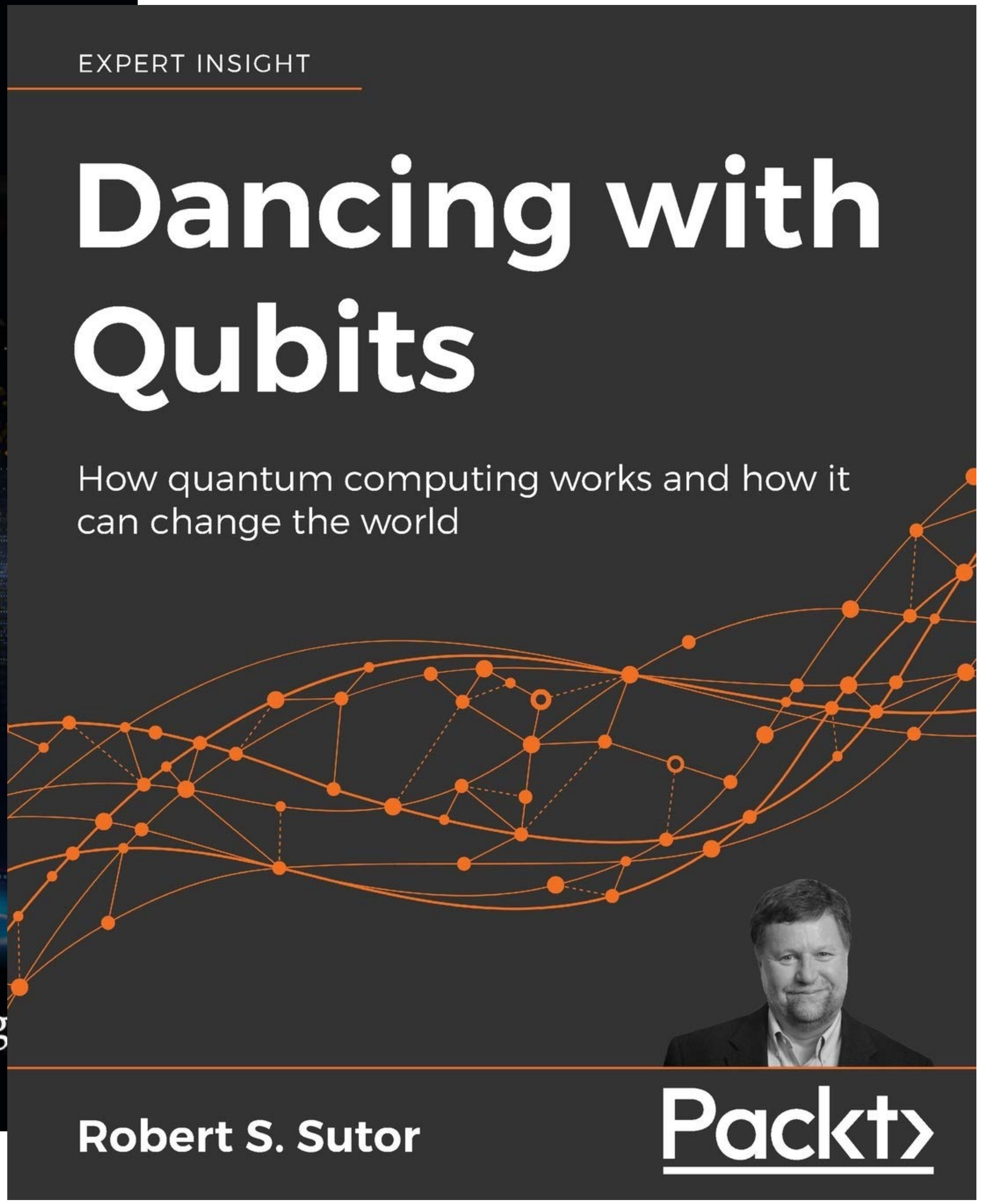

[Electronic Numerical Integrator and Computer - ENIAC]

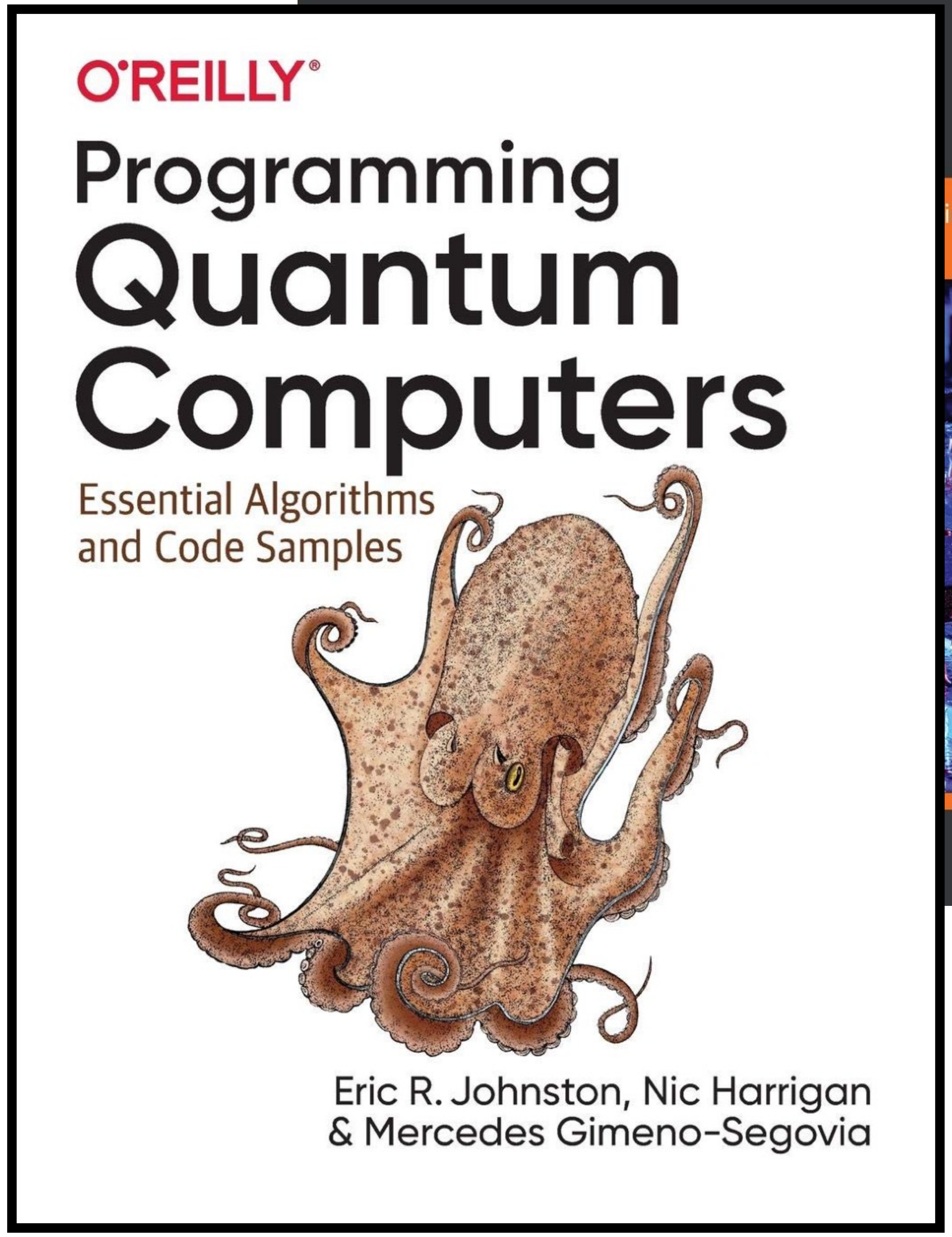
EU Commission Roadmap (Quantum Manifesto)

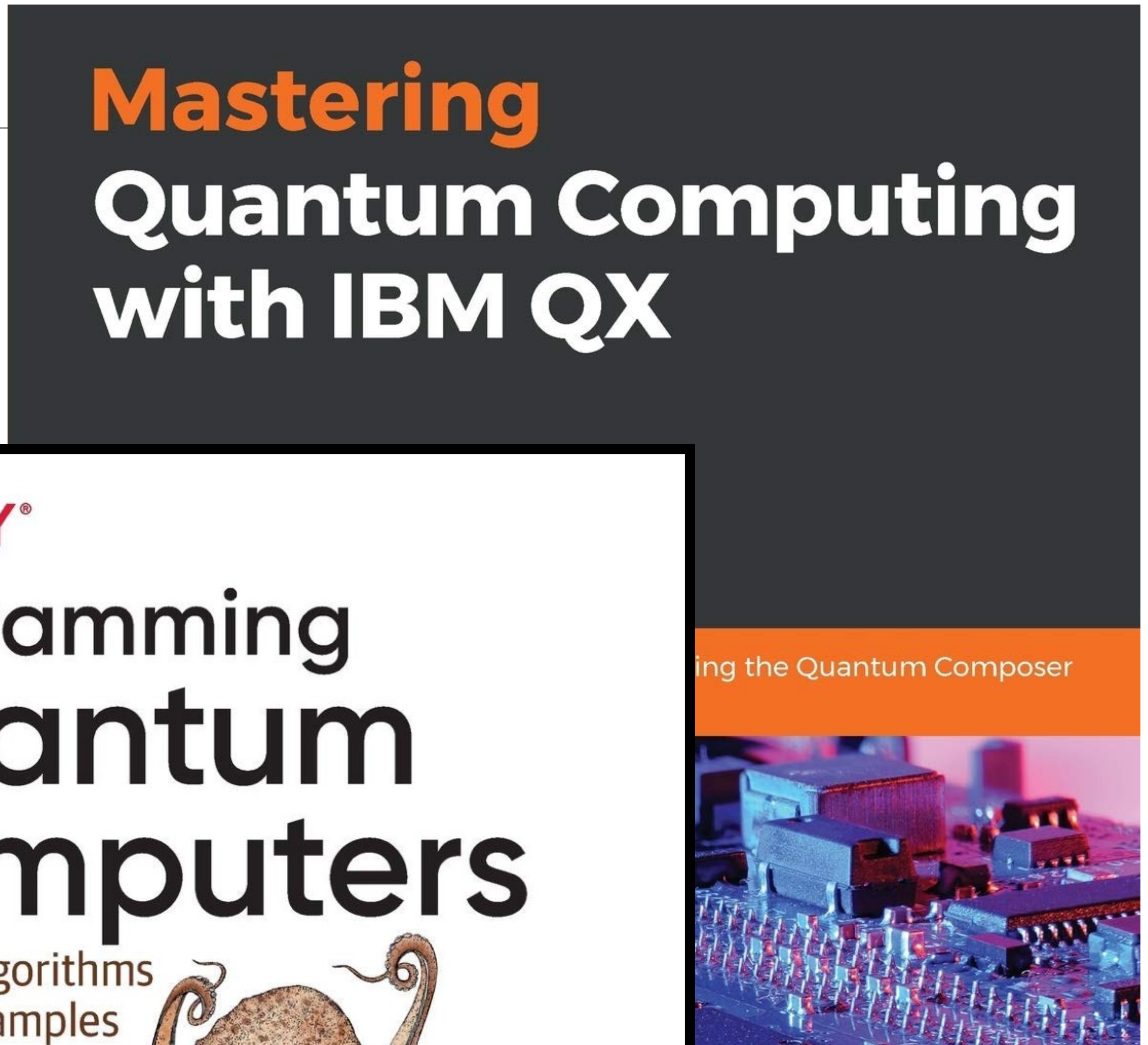


Quantum Computers Going Practical









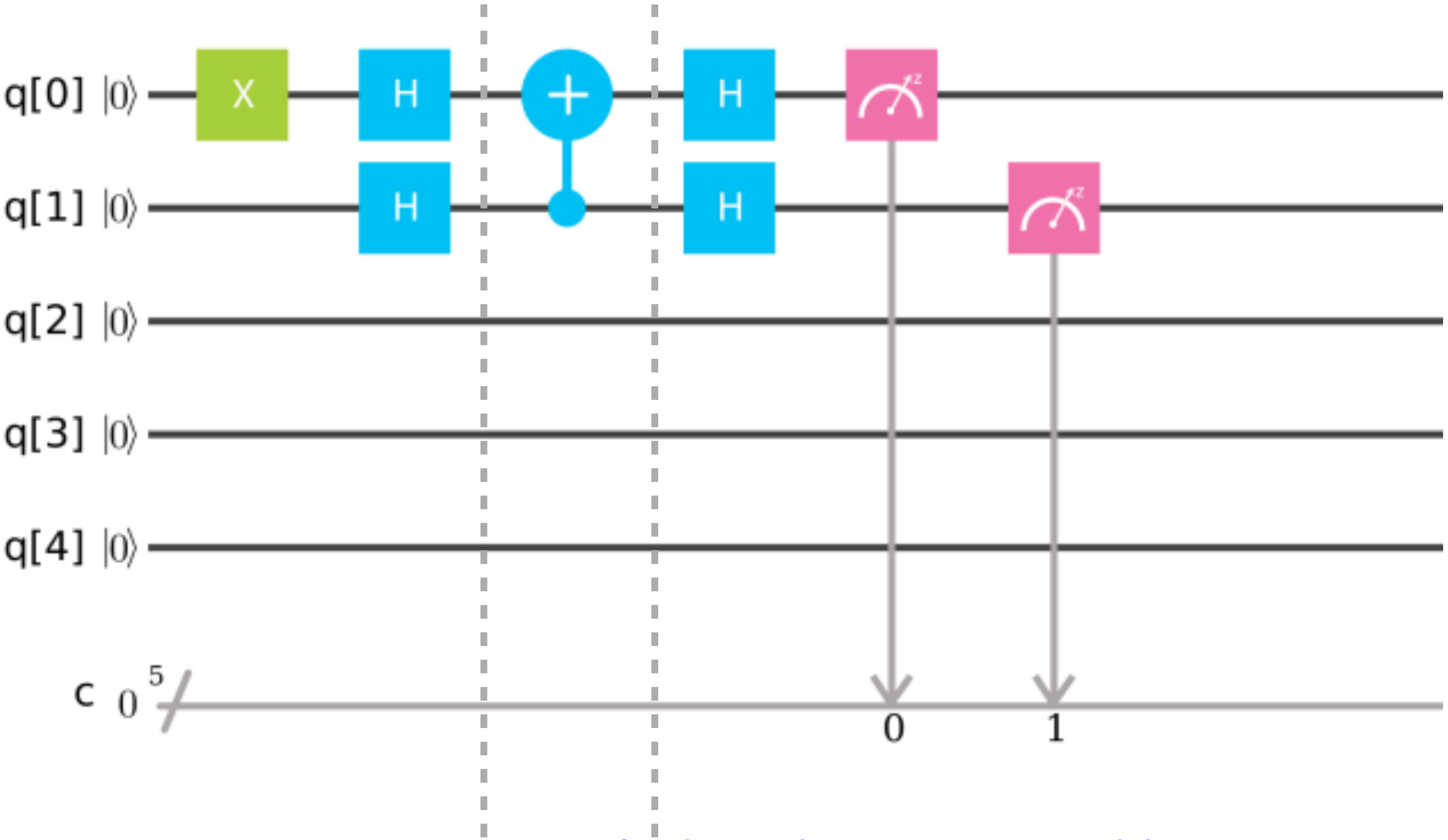
Deutsch-Jozsa: Quantum Computation “Hello World”

- 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* **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 **$2^{N-1} + 1$** 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)

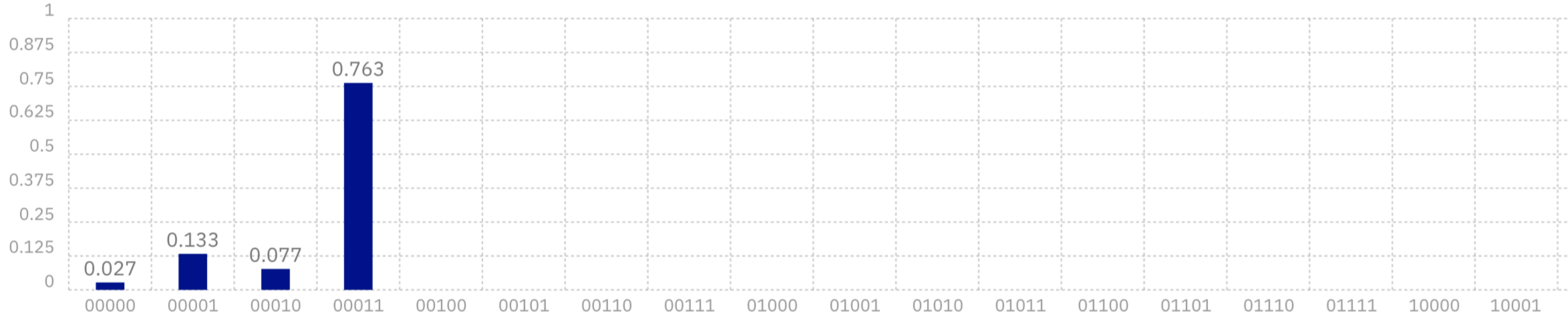


oracle function operator U_f

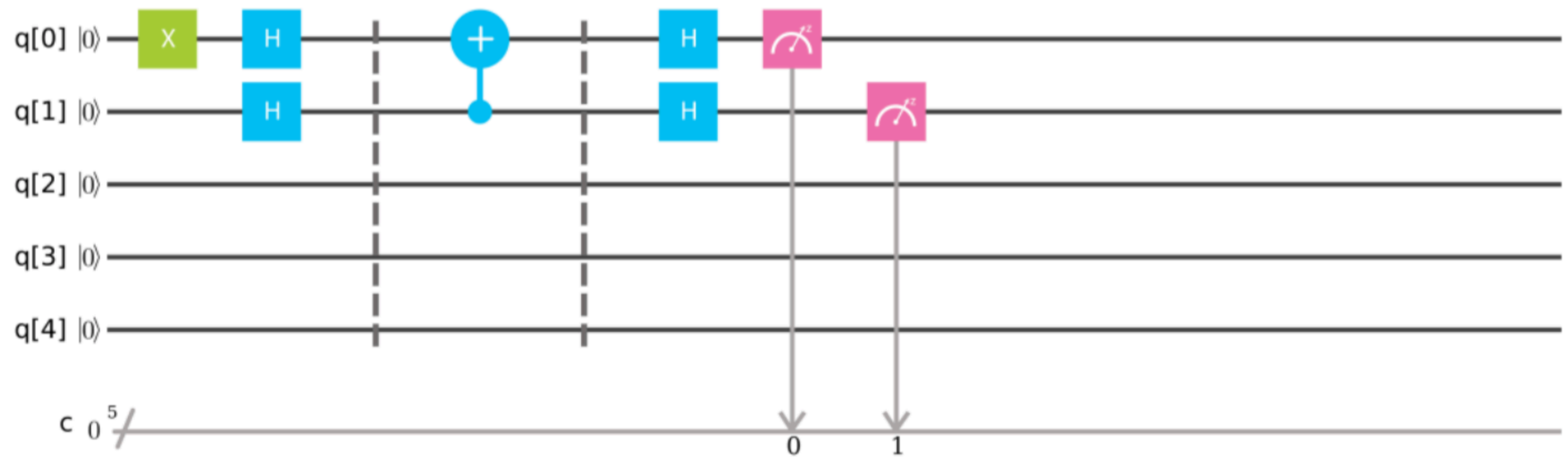
Device: ibmqx4

Quantum State: Computation Basis

Download CSV



Quantum Circuit



OPENQASM 2.0

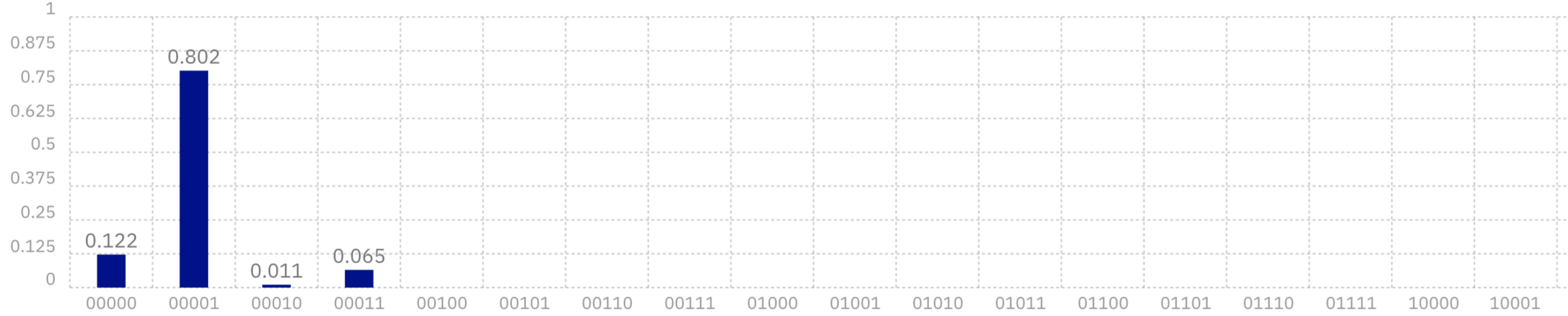
```
include "qelib1.inc";
qreg q[5];
creg c[5];

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

```

Open in Composer

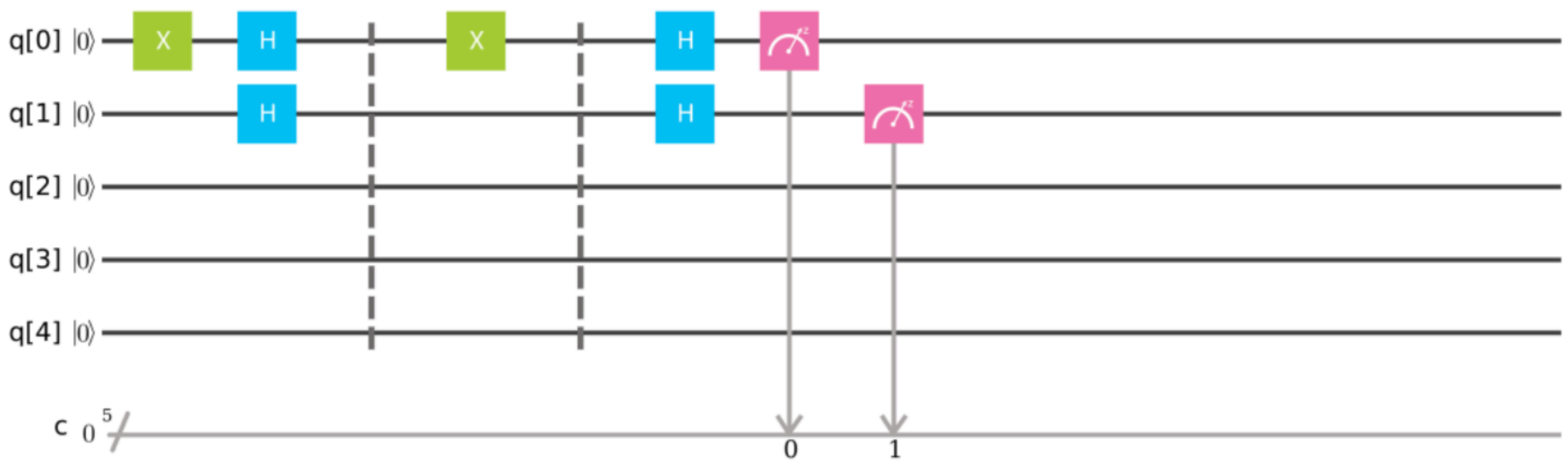
Device: ibmqx4

Quantum State: Computation Basis

Download CSV



Quantum Circuit

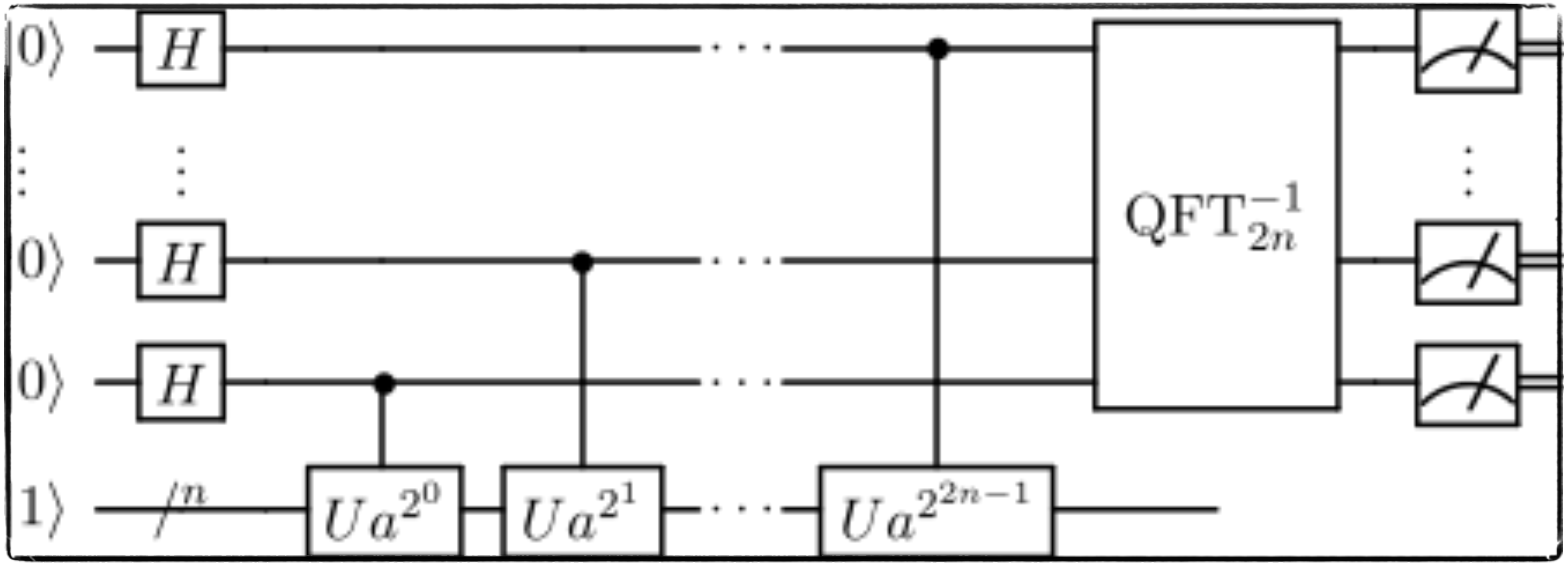


OPENQASM 2.0

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

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

```

Open in Composer

Shor’s Algorithm - Phase Estimation Approach



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 “Cryptocalypse”

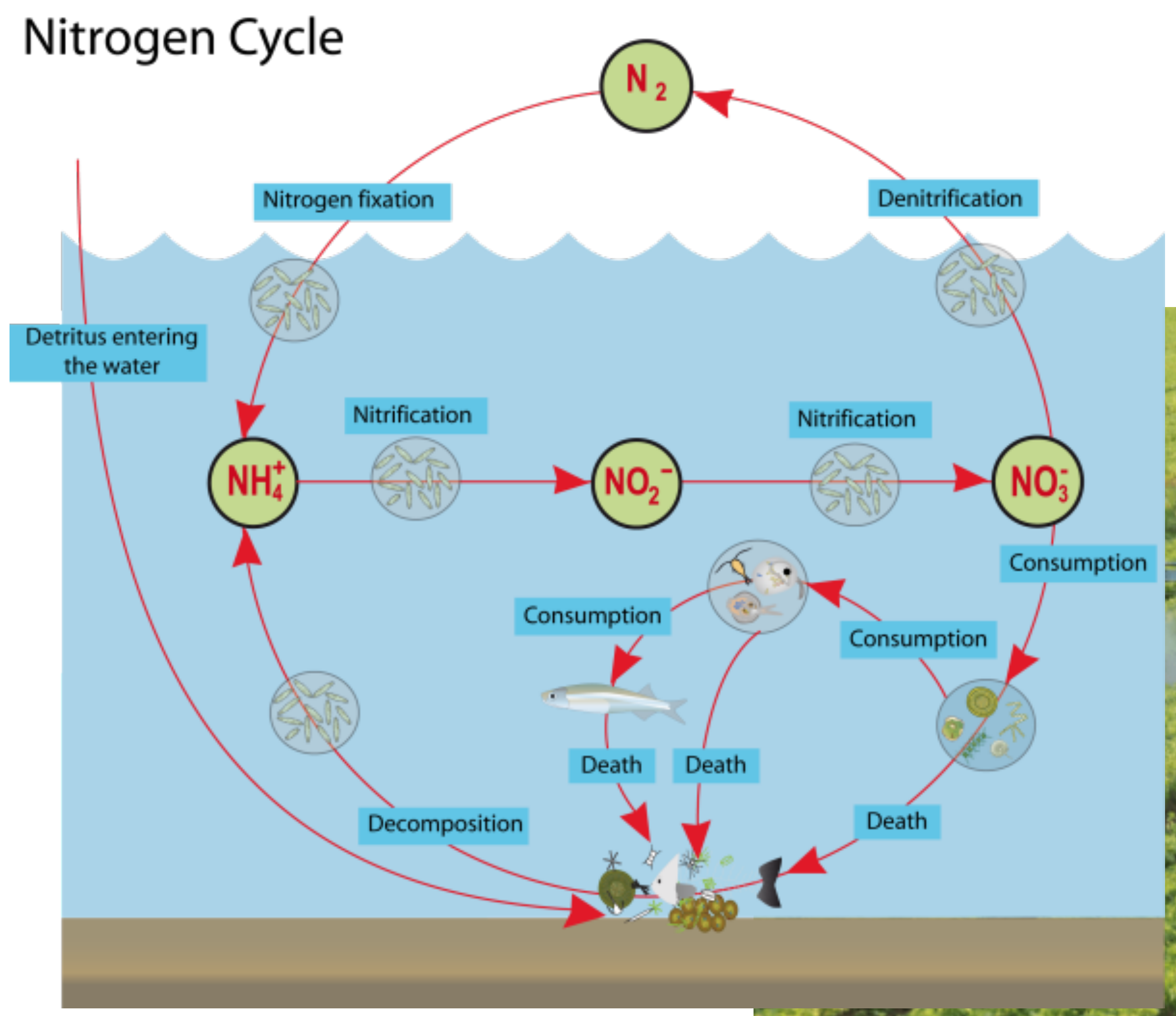
“I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031.”

— Michele Mosca, November 2015

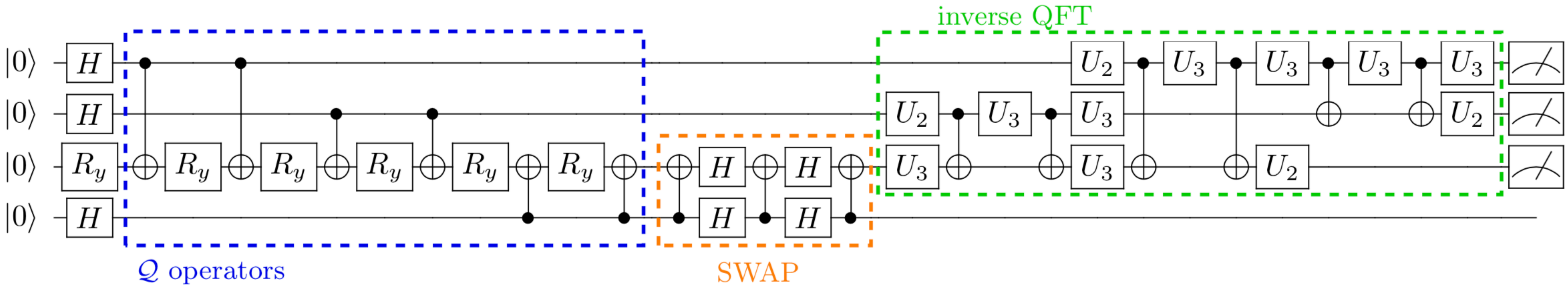
Open Source to Stay Safe for Tomorrow

[https://medium.com/wultra-blog/quantum-resistant-cryptography-introducing-sike-for-java-376d201afa6e]

Peaceful Quantum Computing (chemistry, finance, …)



Value At Risk estimation



Conclusion

- Quantum computing is real
  - we are facing technological and technical issues, but not principal ones
  - we already went a similar way with all the classical computing machinery
- Retroactive cryptanalysis
  - the question of opening today's communication is not if, but when
- Quantum computation is not only a threat
  - QPUs offer promising technological advantages, e.g. for financial analysis