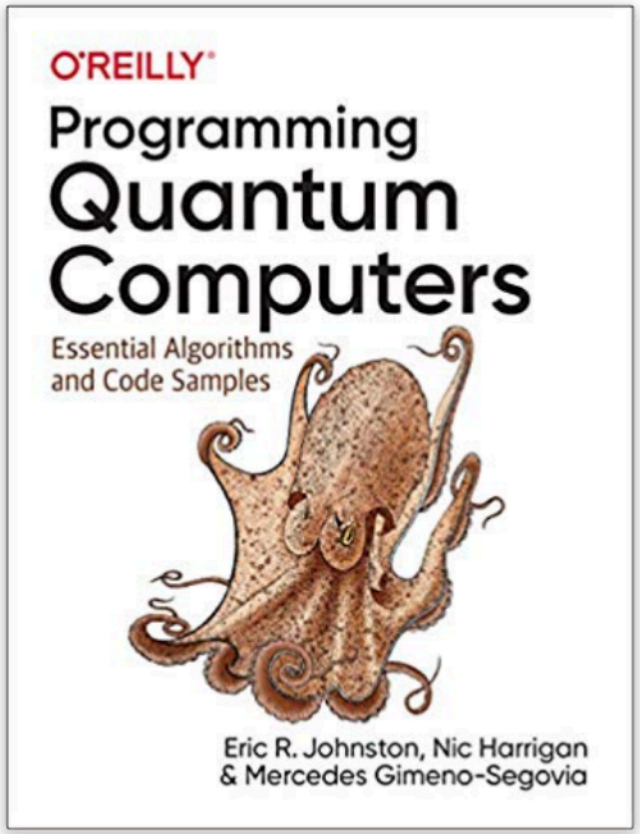
The Advent of Quantum Computers

29.5 – 30.5.2019

Jiří Pavlů and Tomáš Rosa
Cryptology and Biometrics Competence Centre of Raiffeisen BANK International



See this image

Programming Quantum Computers: Essential Algorithms and Code Samples

Paperback – 31. August 2019

by Eric R. Johnston (Autor), Nic Harrigan (Autor), Mercedes Gimeno-Segovia (Autor)

› See all formats and editions

Paperback
EUR 66.99

Promotion Message Vorbesteller-Preisgarantie 1 promotion

This item can be delivered to Czech Republic. Details

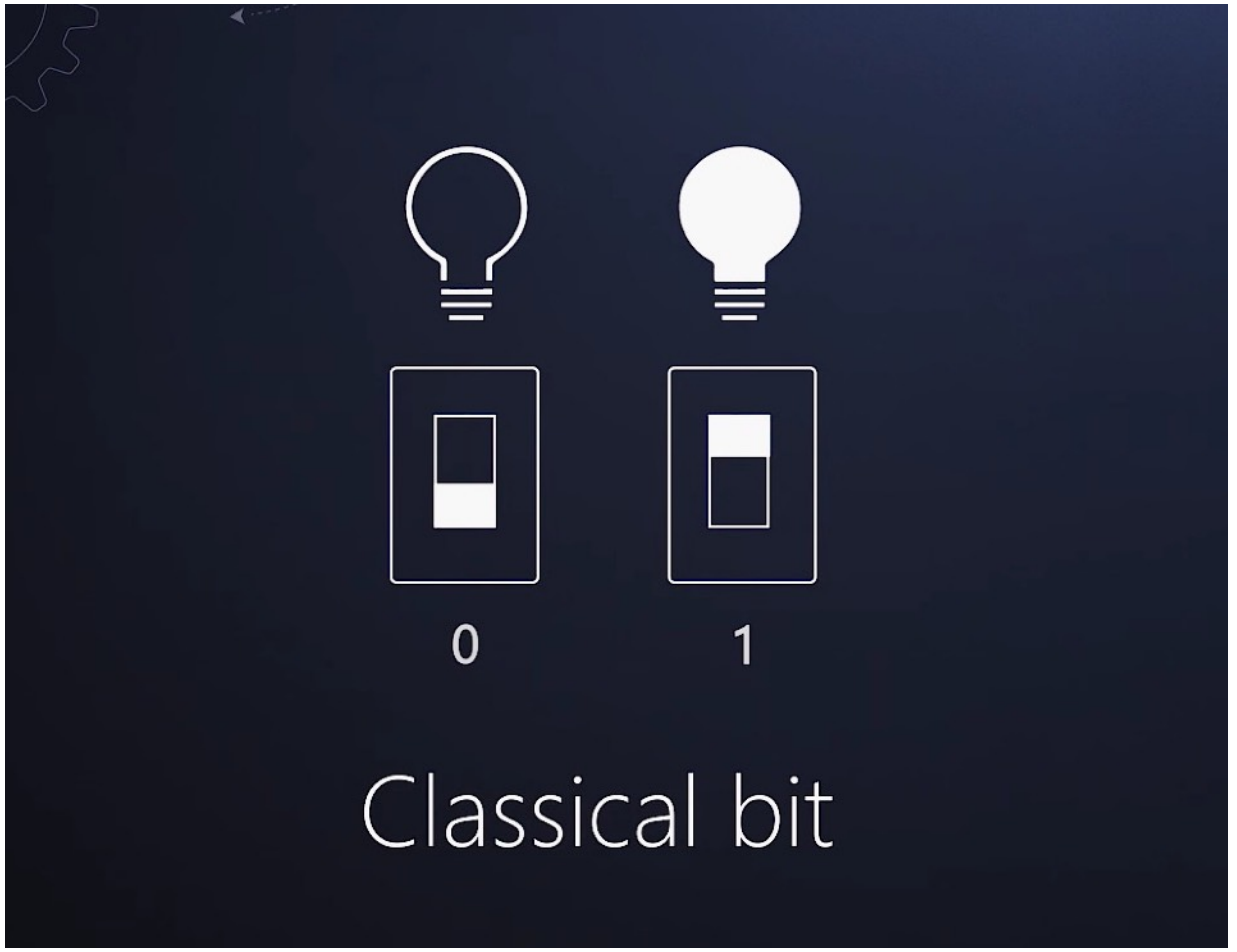
1 New from EUR 66.99

Quantum computers are set to kick-start a second computing revolution in an exciting and intriguing way. Learning to program a Quantum Processing Unit (QPU) is not only fun and exciting, but it's a way to get your foot in the door. Like learning any kind of programming, the best way to proceed is by getting your hands dirty and diving into code.

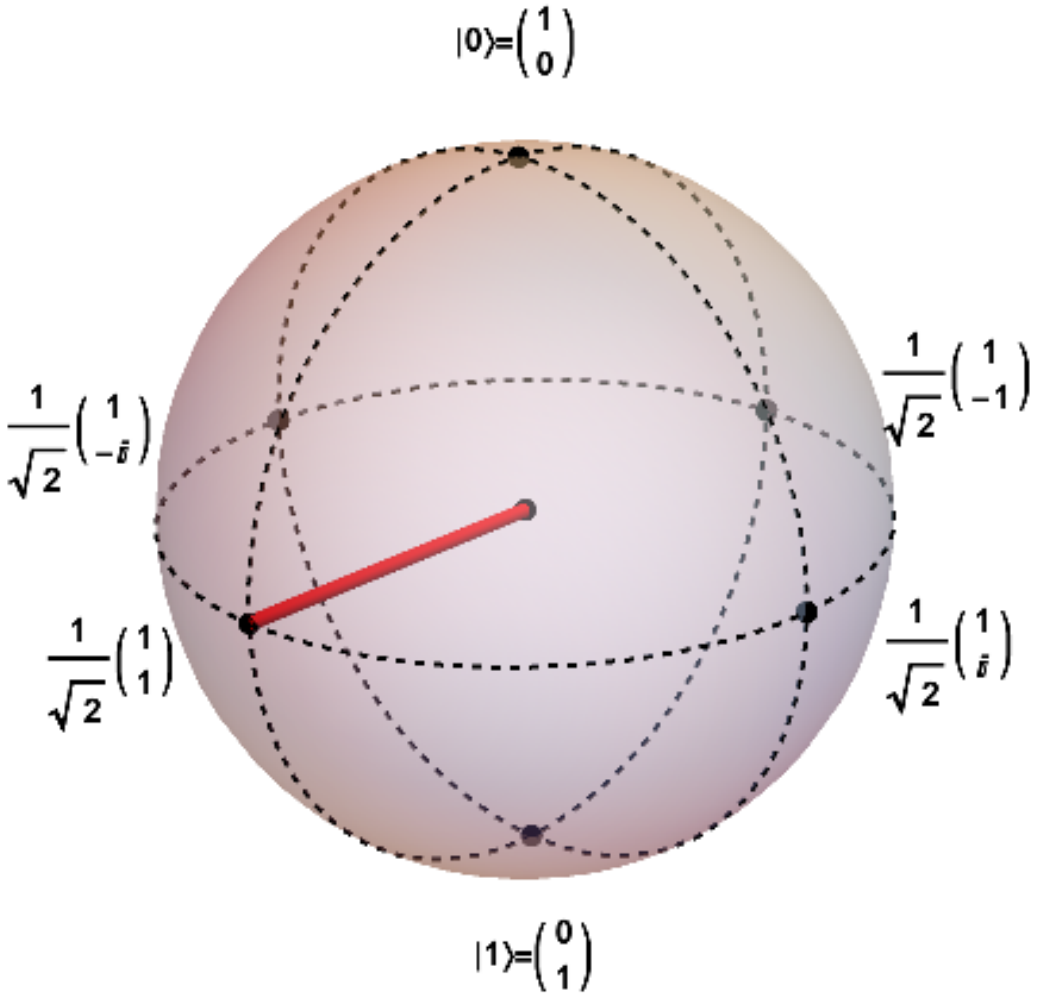
This practical book uses publicly available quantum computing engines, clever notation, and a programmer's mindset to get you started. You'll be able to build up the intuition, skills, and tools needed to start writing quantum programs and solve problems that you care about.

› Read less

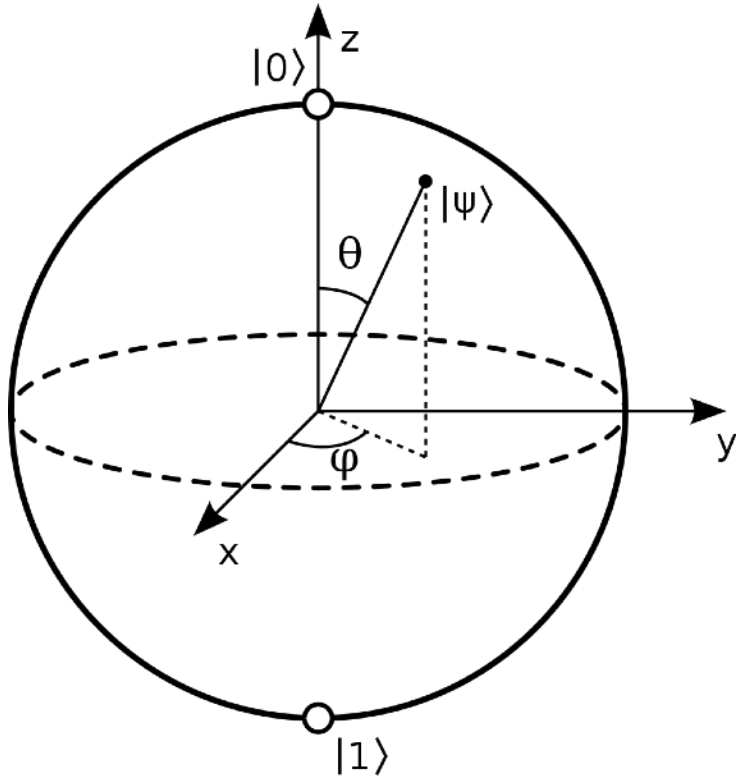
Classical Computer - Classical Bit



Quantum Computer - Quantum Bit (Qubit)



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



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

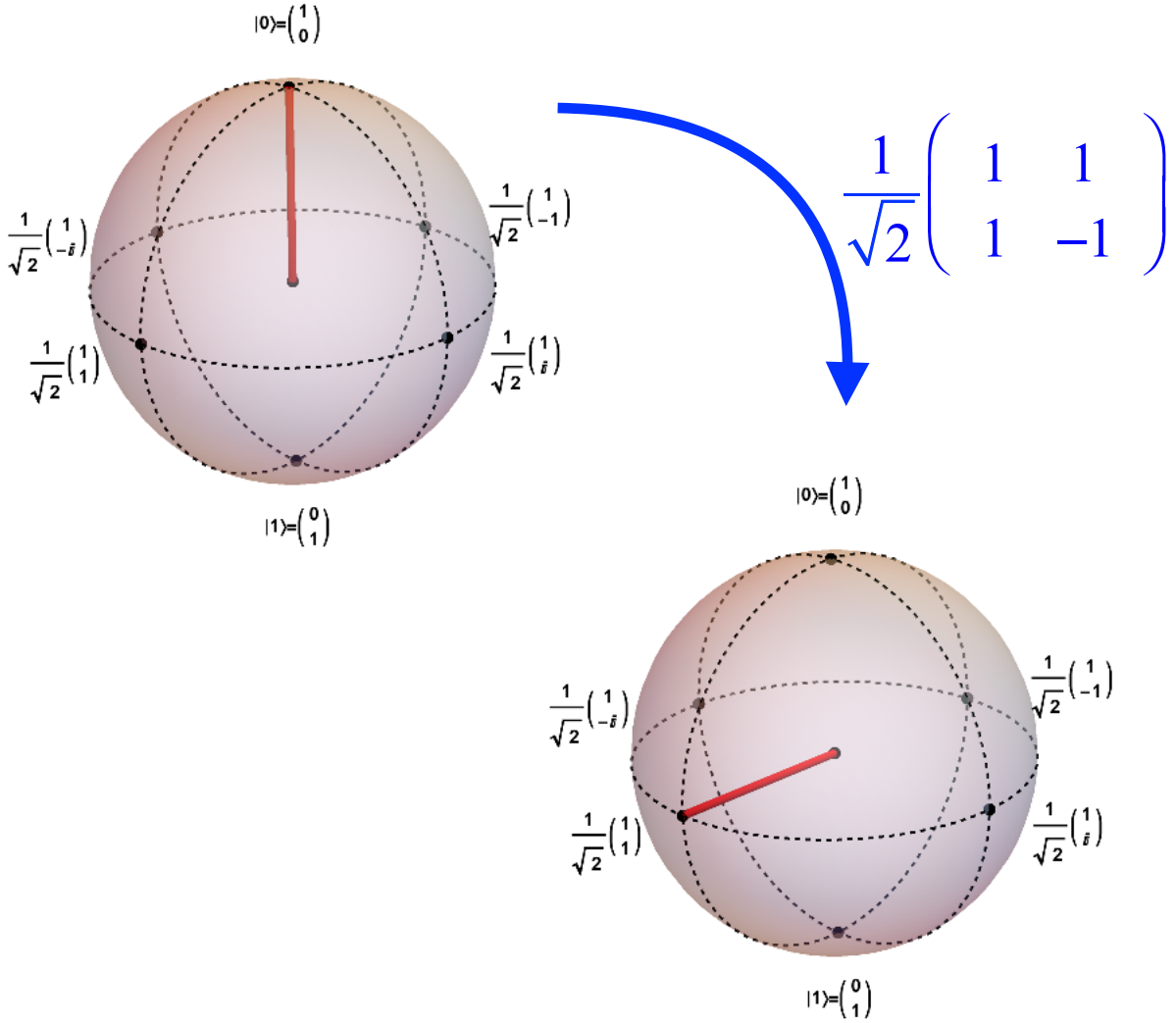
$$|\omega_0|^2 + |\omega_1|^2 = 1$$

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

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

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

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



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.

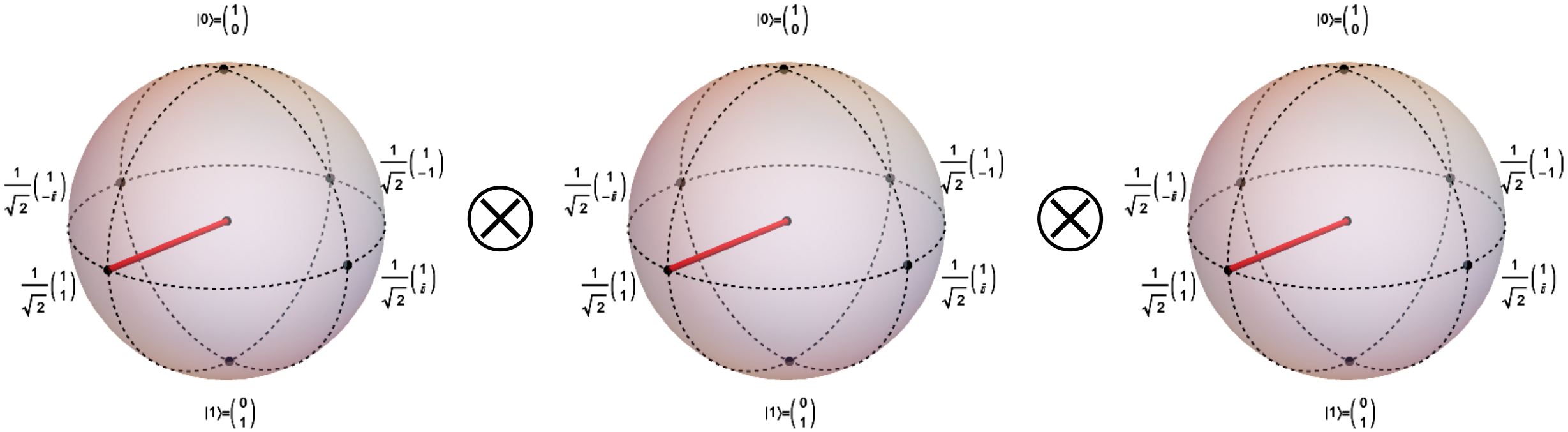
    - together with linear operators acting on this register, this is the source of so-called **quantum parallelism**

    - 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…)



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

Computational Aspects

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

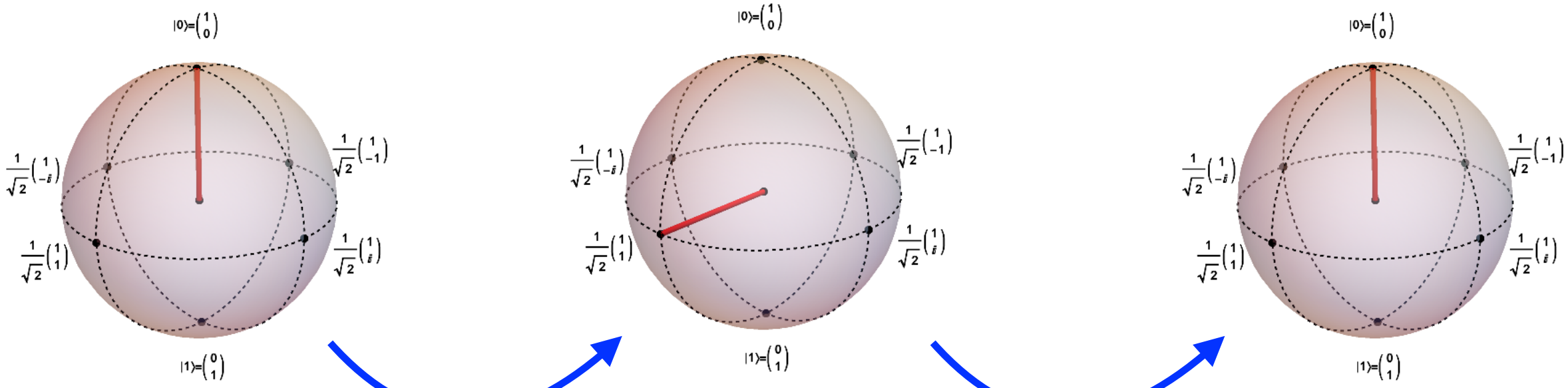
- We can continue further to derive computational paradigms. For instance:

    - quantum parallelism (already noted above)

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

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

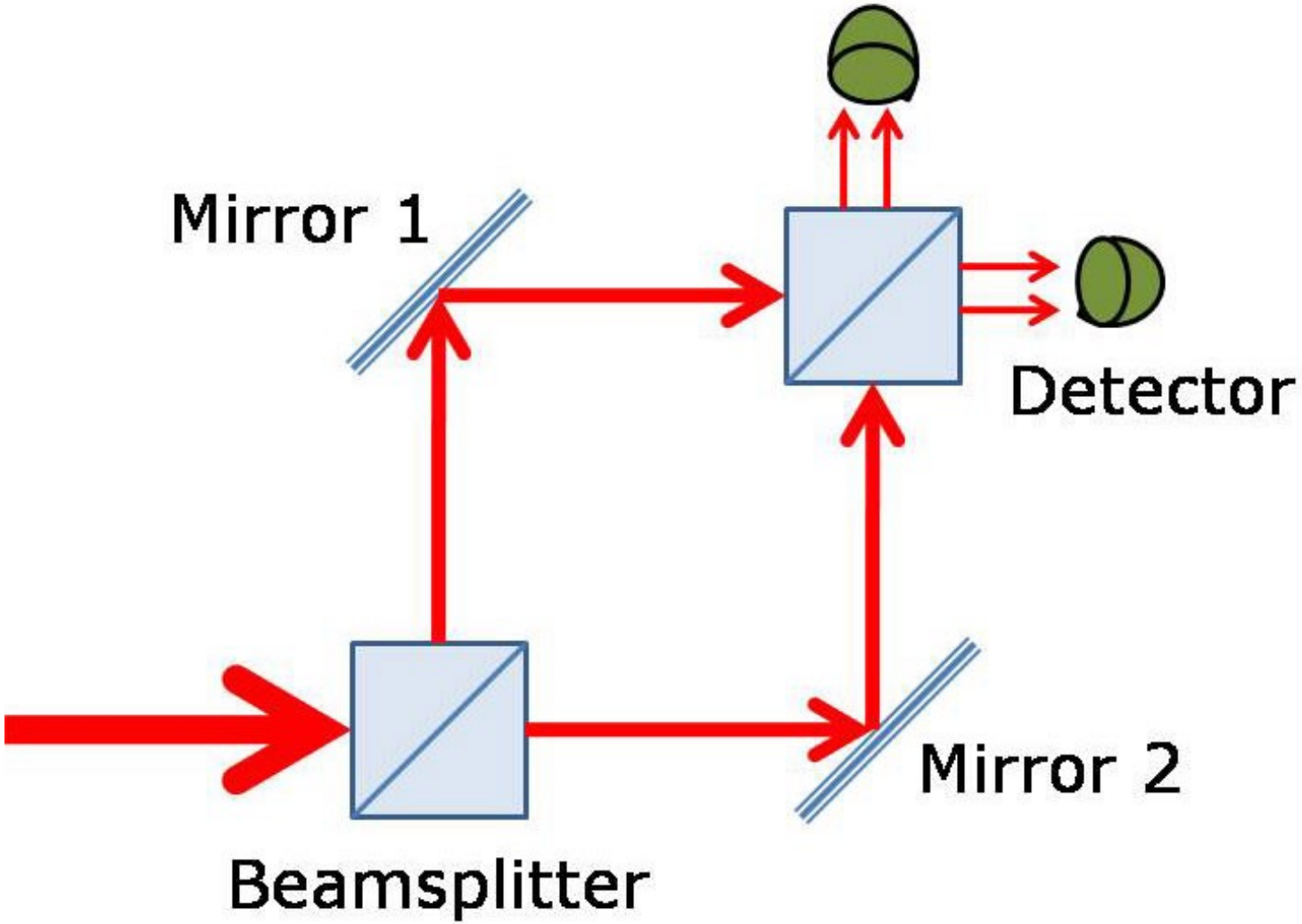
Computational Interference



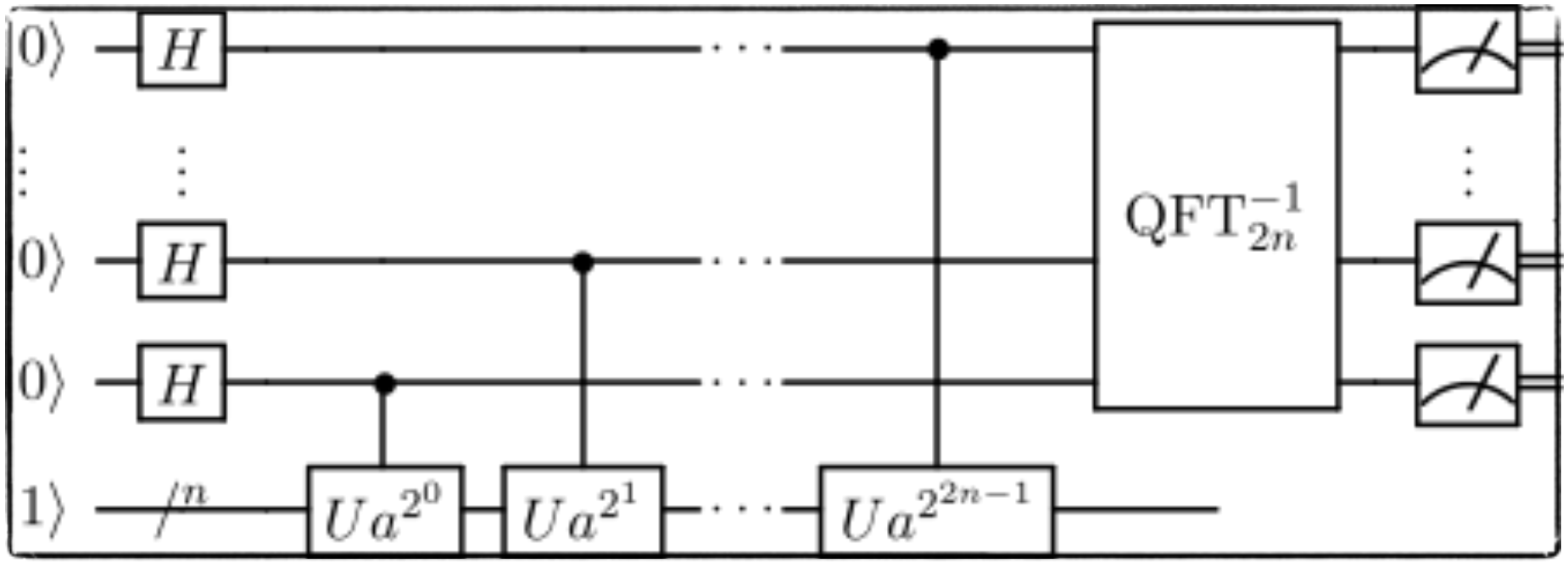
$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

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

This was just a computational version of Mach-Zehnder experiment



Shor's Algorithm



Consider the Quantum Register

$$|\psi\rangle = |k\rangle |a^k \bmod N\rangle$$

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

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

Superposing QFT

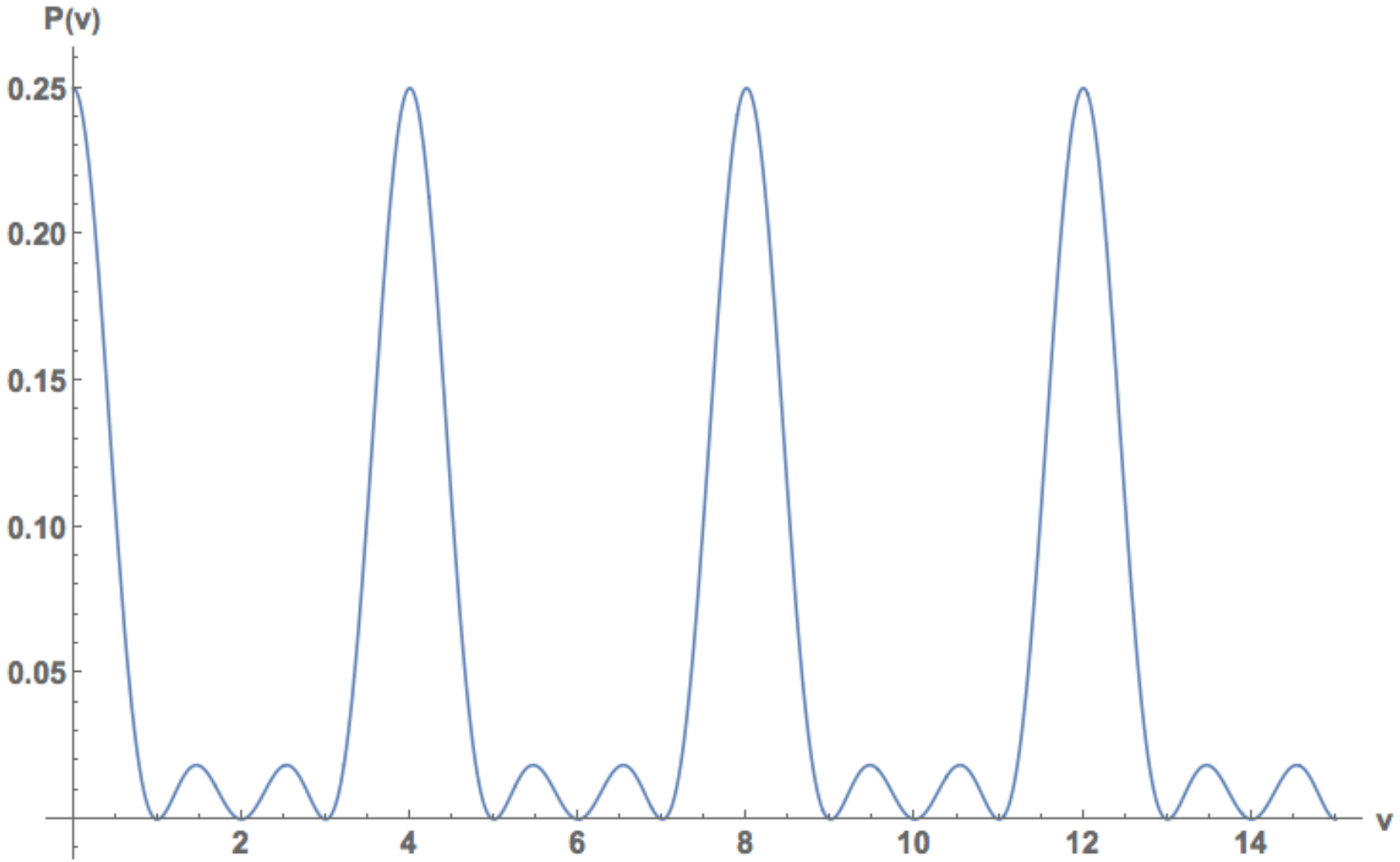
$$\sum_{(u)} \left| ur + k \right\rangle \left| a^k \right\rangle \rightarrow \frac{1}{\sqrt{m}} \sum_{(u)} \sum_{v=0}^{m-1} e^{\frac{2\pi i (ur+k)v}{m}} \left| v \right\rangle \left| a^k \right\rangle$$

$$= \frac{1}{\sqrt{m}} \left[\underbrace{\sum_{v=0}^{m-1} e^{\frac{2\pi i k v}{m}}} \left(\underbrace{\sum_{(u)} e^{\frac{2\pi i u v}{\frac{m}{r}}}} \left| v \right\rangle \left| a^k \right\rangle \right) \right]$$

fixed phase swallow

interference control

Exploiting the Parallelism via QFT Interference



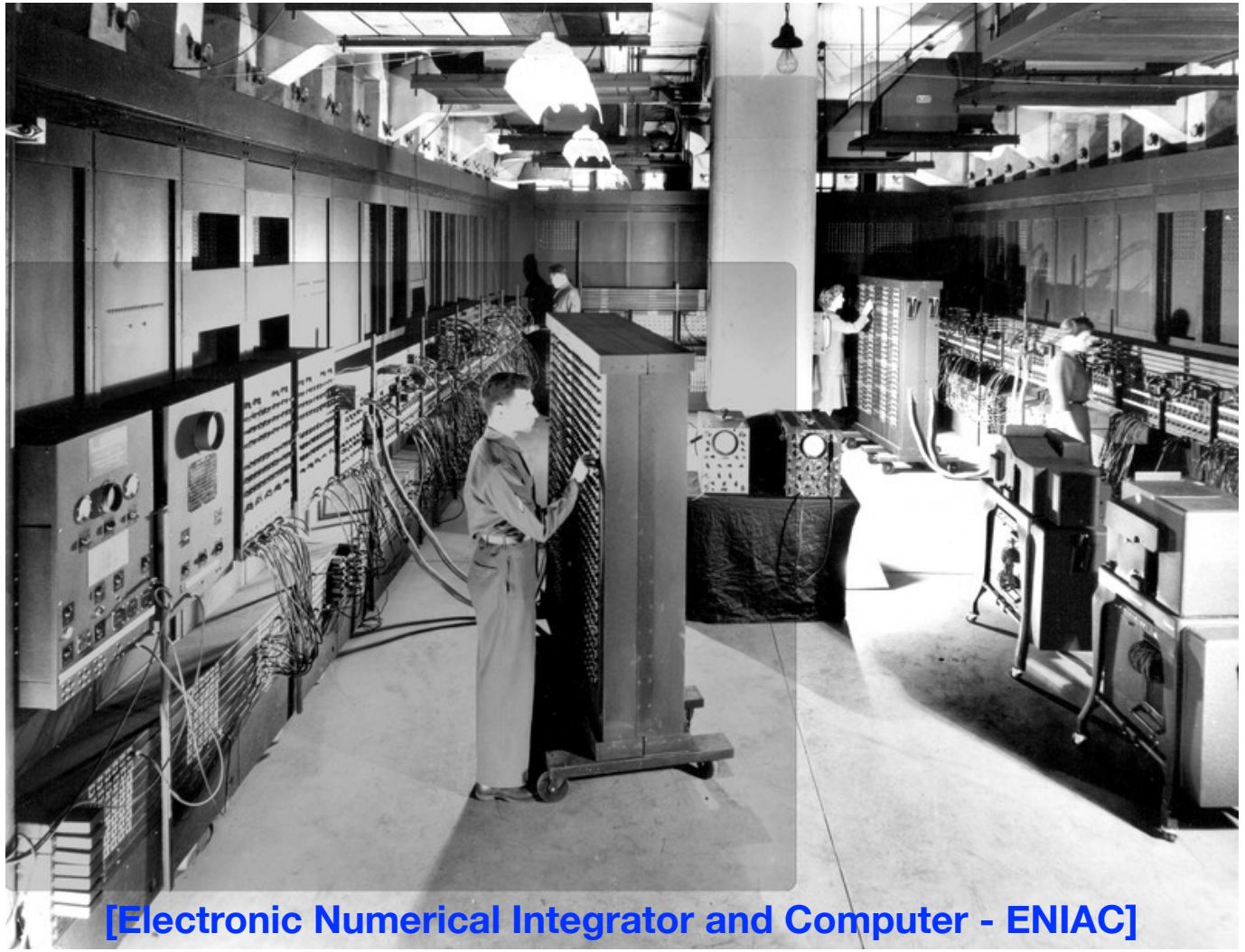
It is not only about the Shor's algorithm

- **Grover's search method**
  - quadratic speed-up, usable for both asymmetric and symmetric algorithms
- **Simon's period finding (also with Bernstein-Vazirani core)**
  - 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

Main Challenges for Quantum Computers Today

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



[Electronic Numerical Integrator and Computer - ENIAC]

“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.*

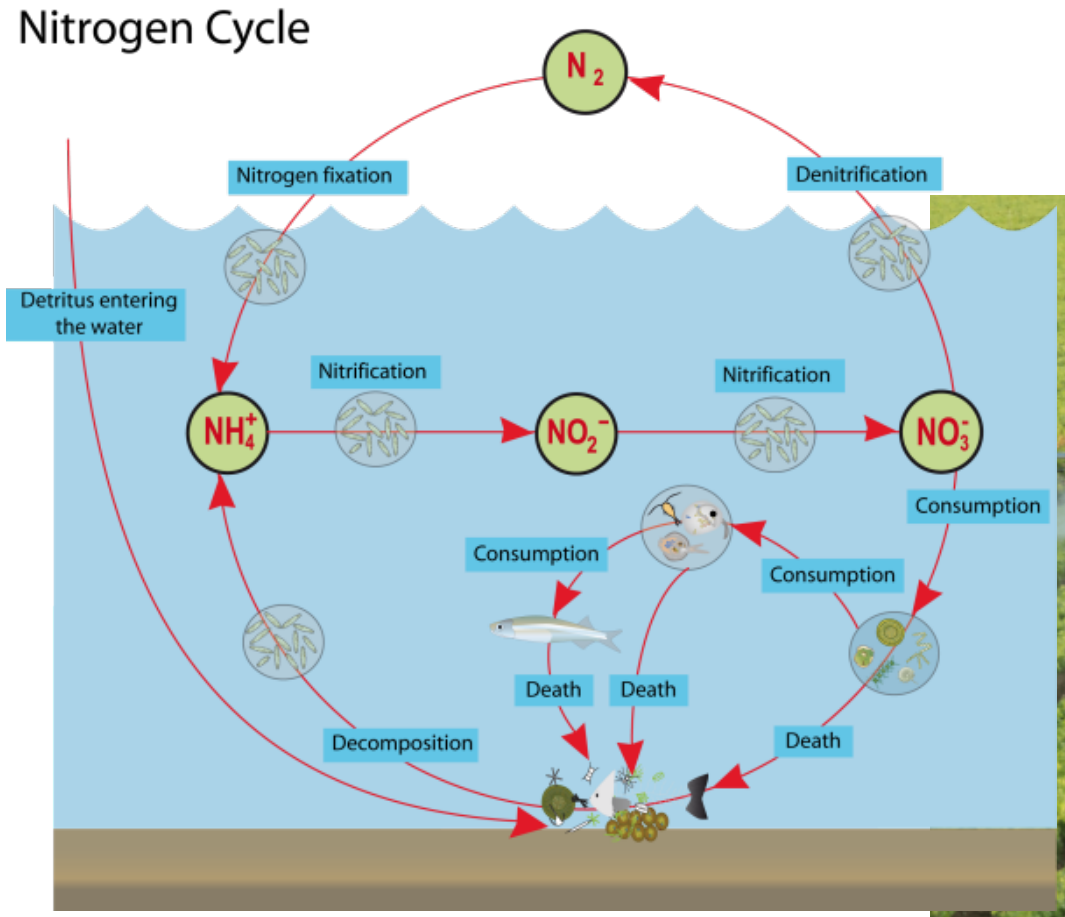
— http://nap.edu/25196

“Quantum Computing: Progress and Prospects”

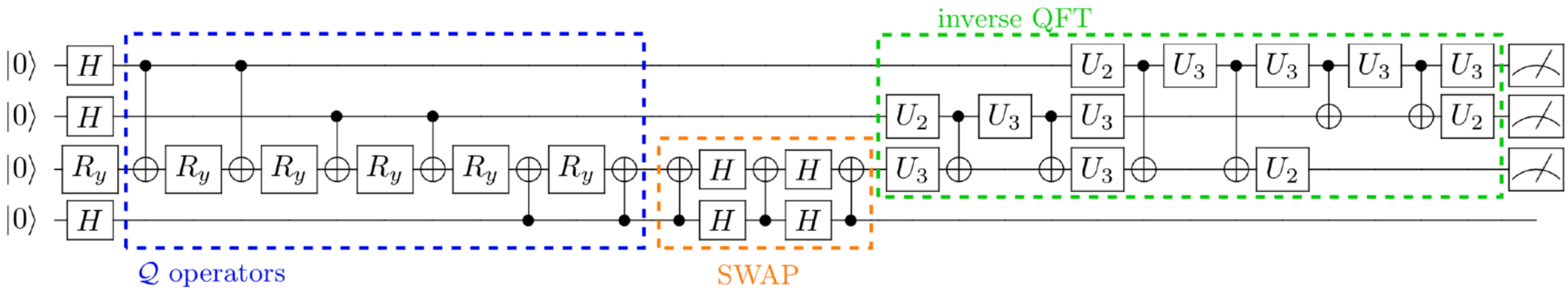
Key Finding 10: *Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development,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

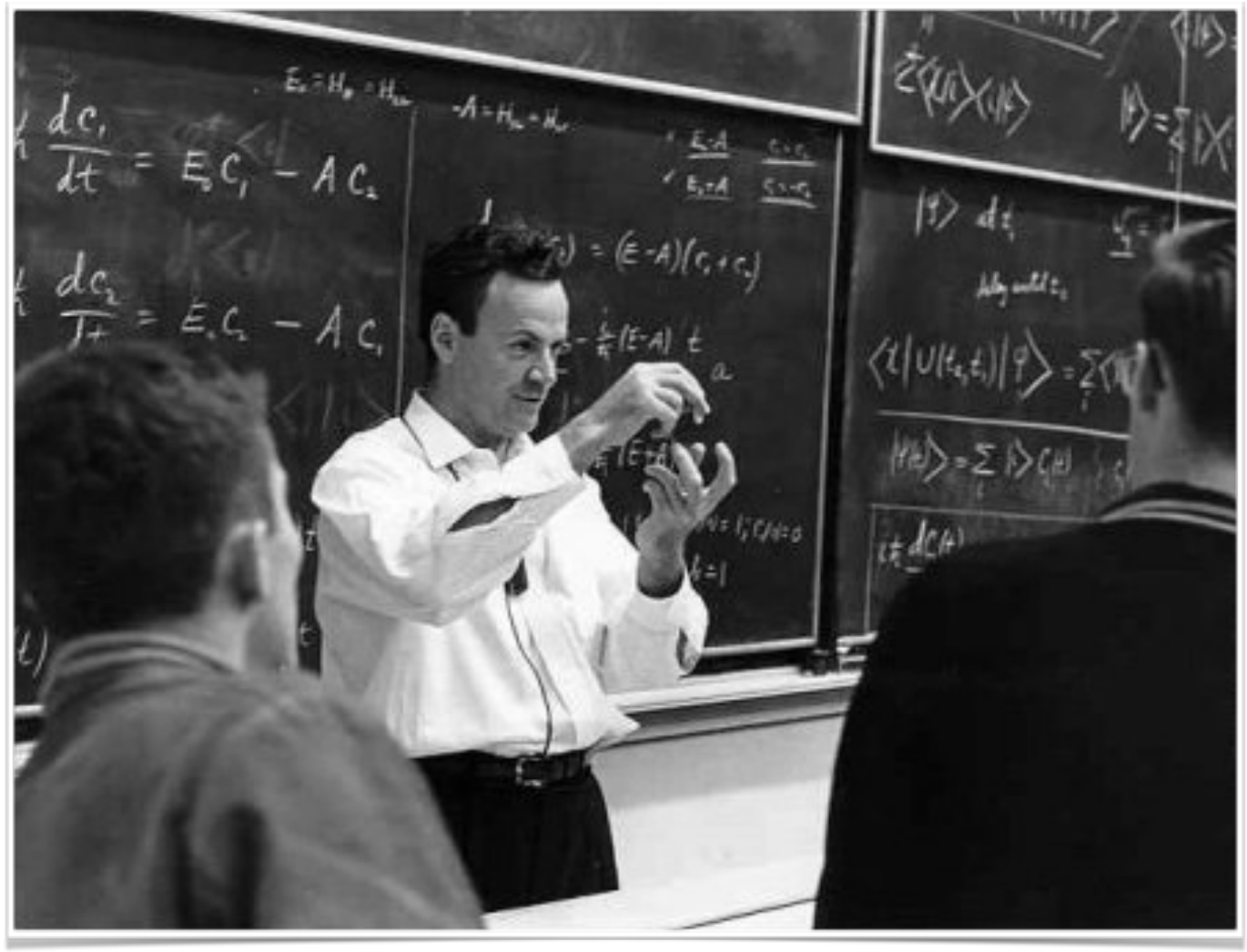
— http://nap.edu/25196

Peaceful Quantum Computing



Value at Risk Estimation





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)