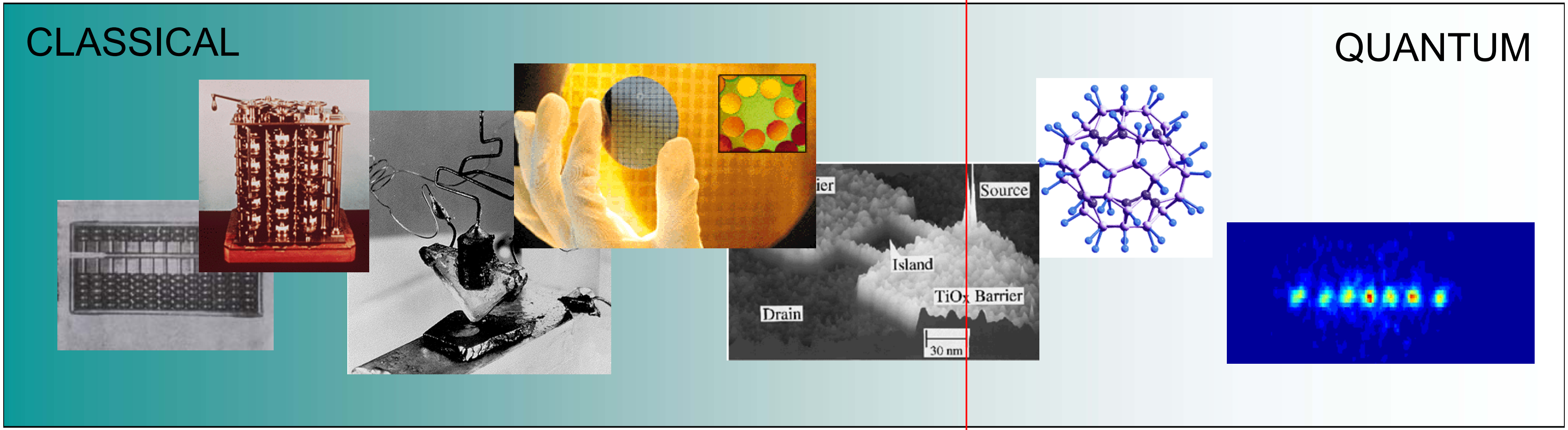
NUS
National University
of Singapore

UNIVERSITY OF
CAMBRIDGE

Quantum Information Science Revisited

Artur Ekert

WHY QUANTUM INFORMATION ?

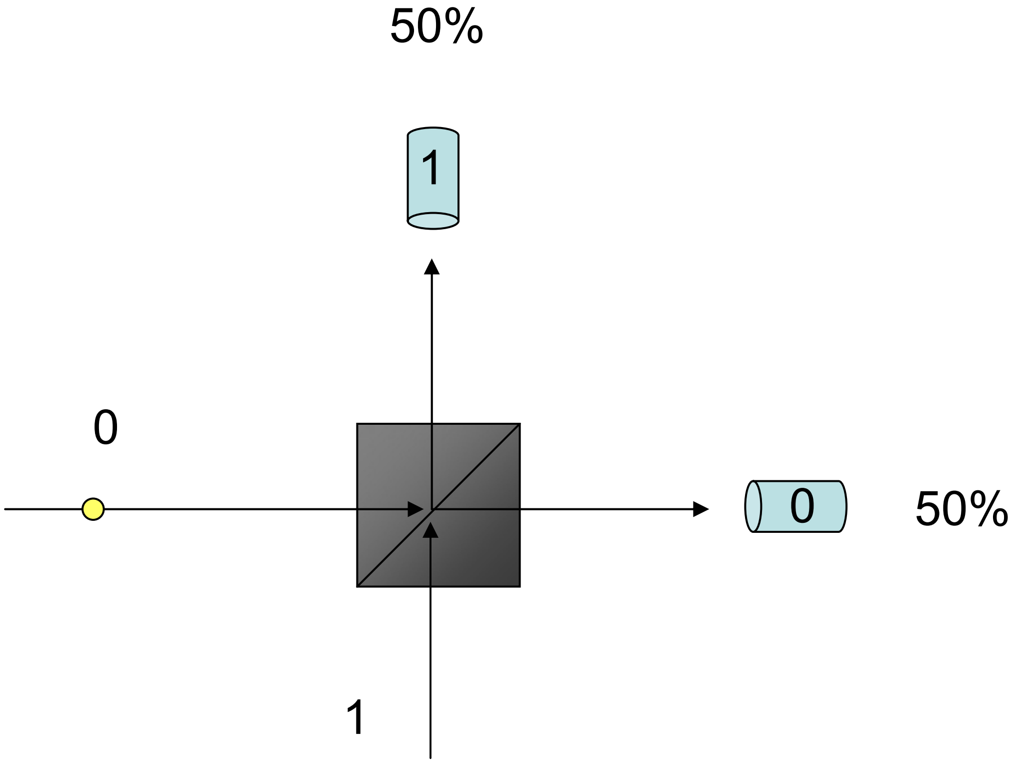


Technology	**Moor’s law**
Computer Science	**computational complexity**
Physics	**refutation of quantum theory**
Mathematics & Logic	**physics and mathematics**

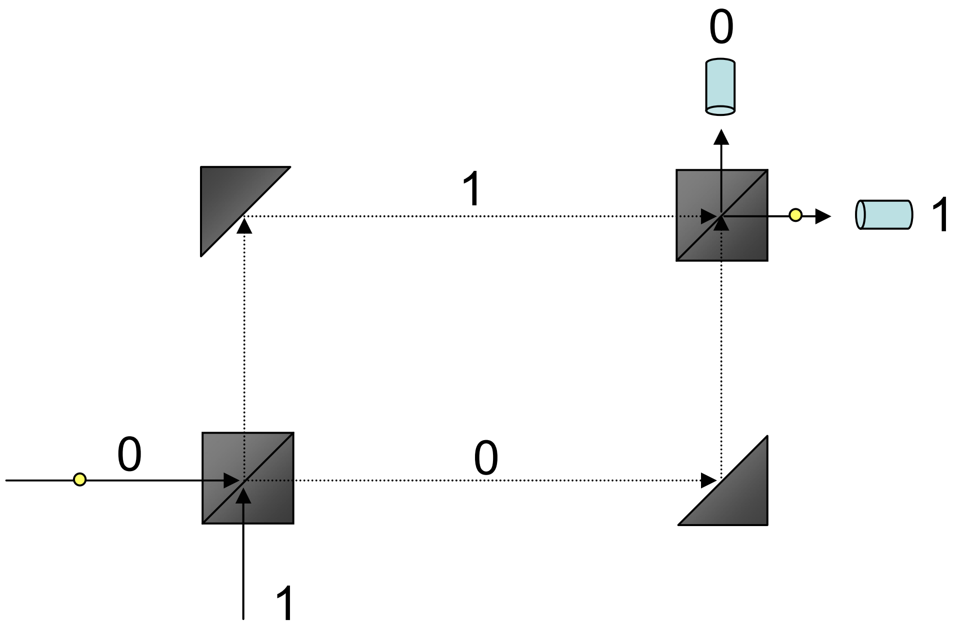
There is no information without physical representation

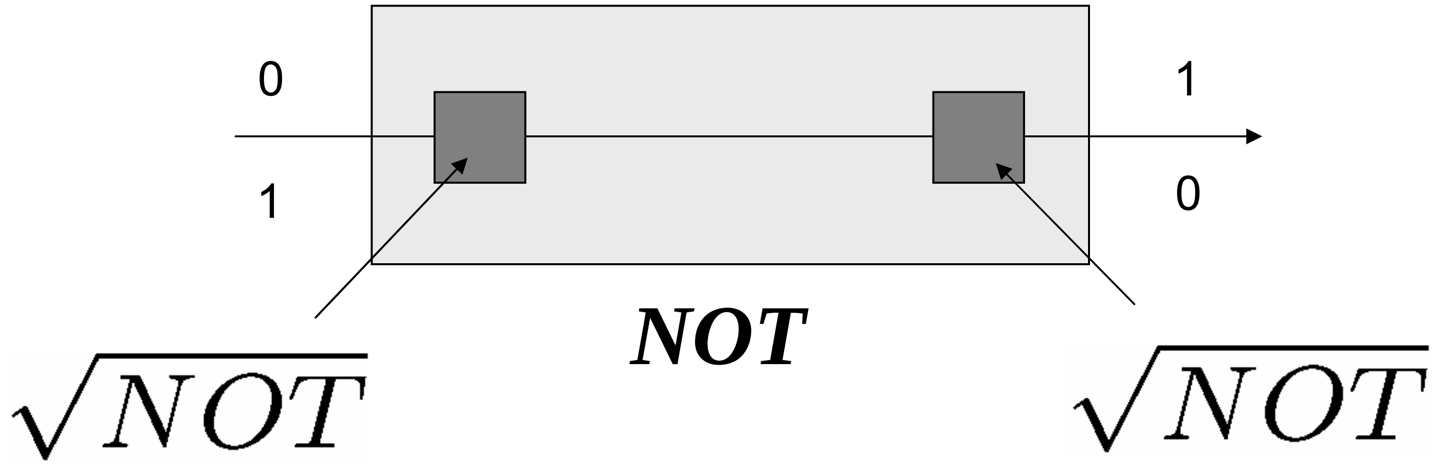
There is no information processing without a physical process

What is so special about quanta?

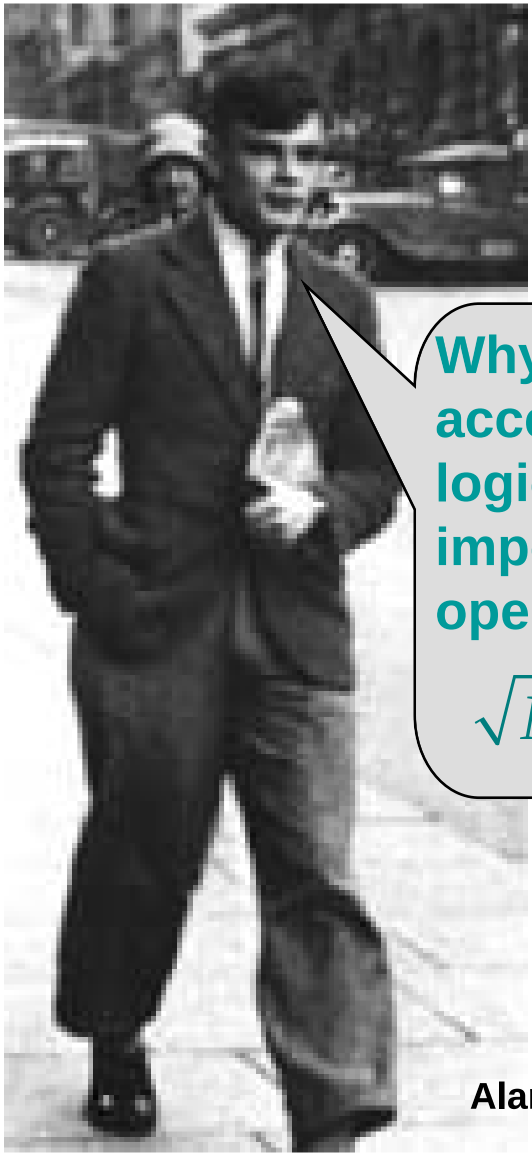


They defy common logic





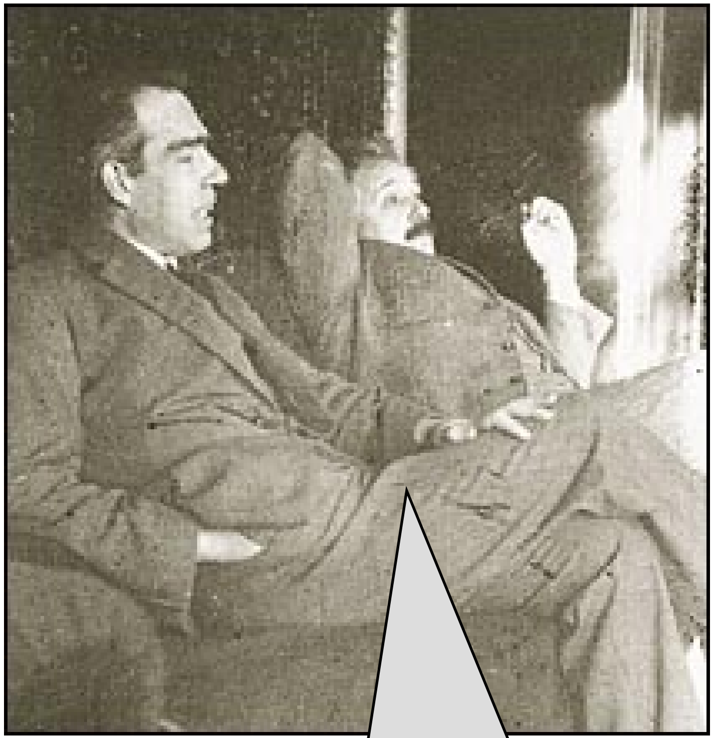
Logic or Physics?



Alan Turing

Why shall I accept this logically impossible operation

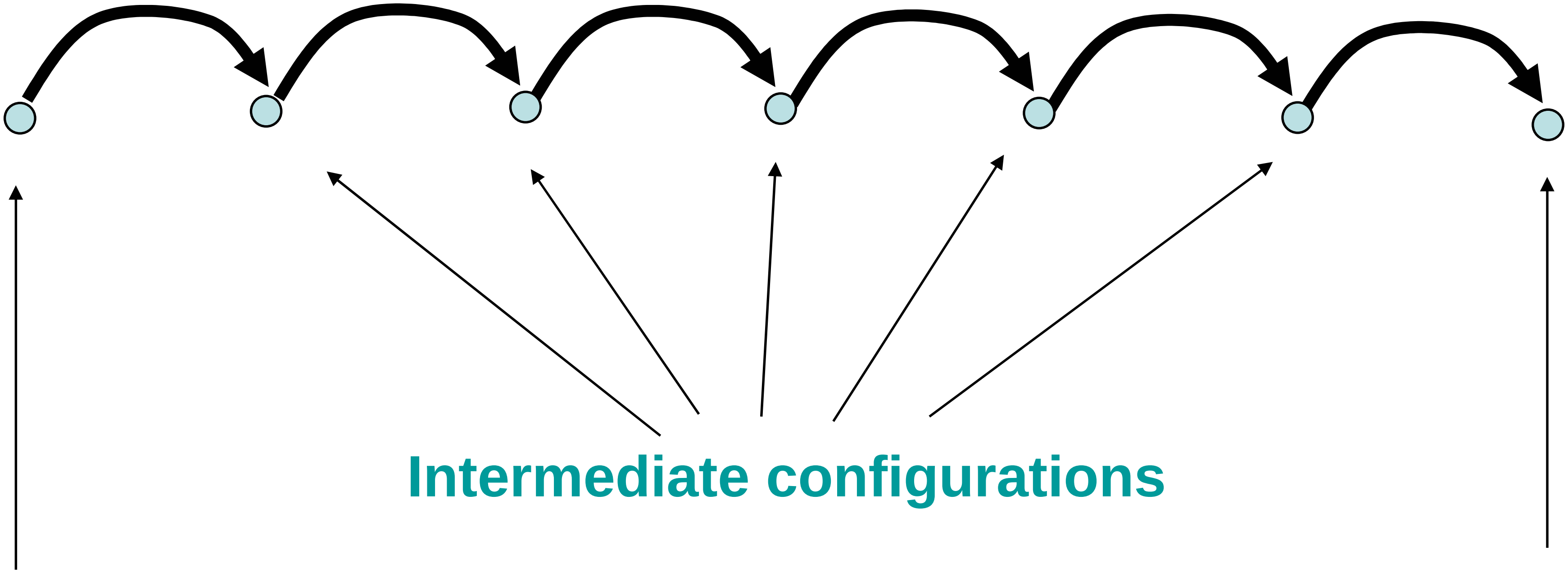
$\sqrt{NOT}$?



Niels Bohr &
Albert Einstein

Because its physical representation does exist in Nature!
It can be performed!

Deterministic Turing computation

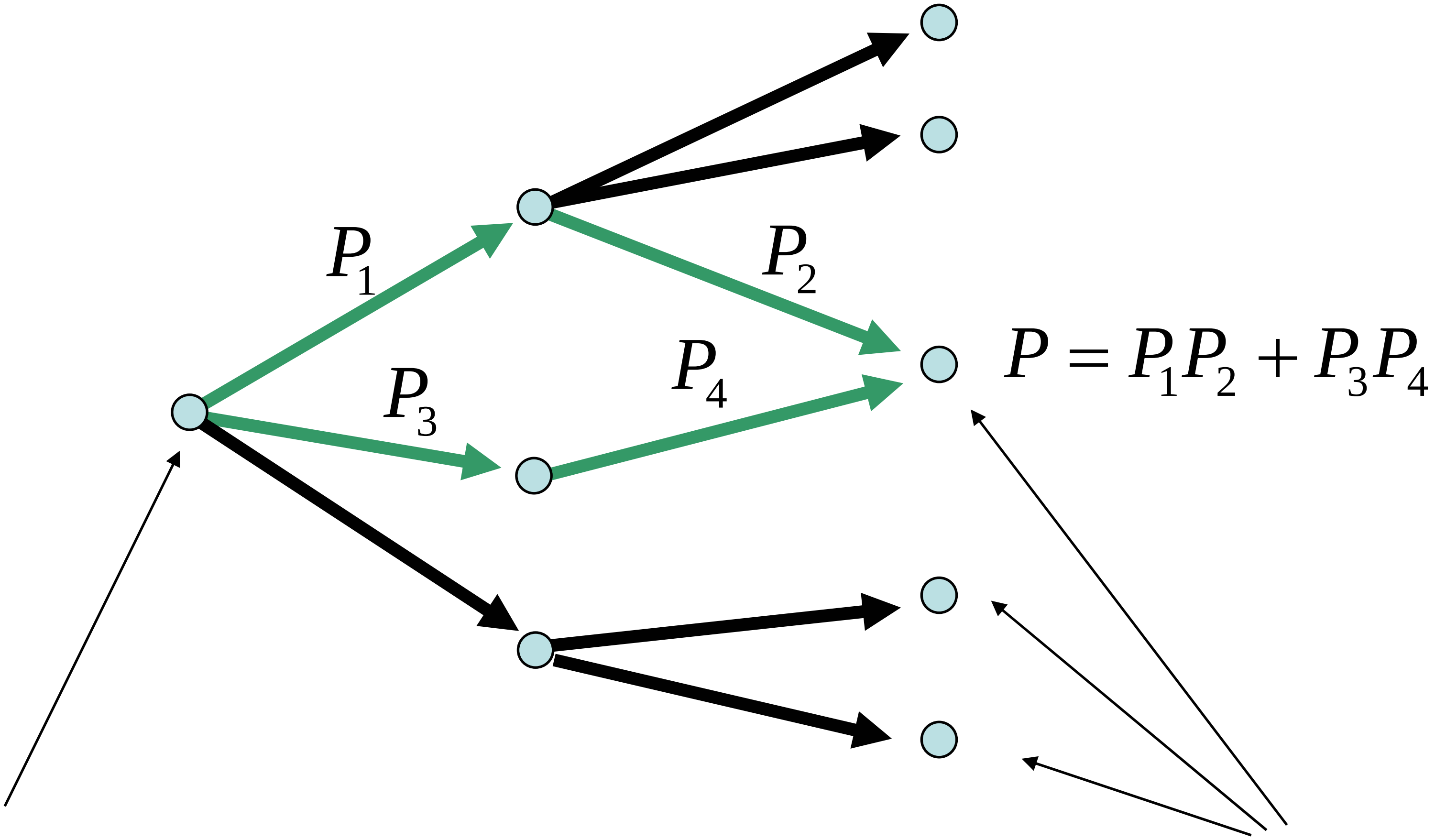


Intermediate configurations

Initial configuration (input)

Final configuration (output)

Classical probabilistic computation

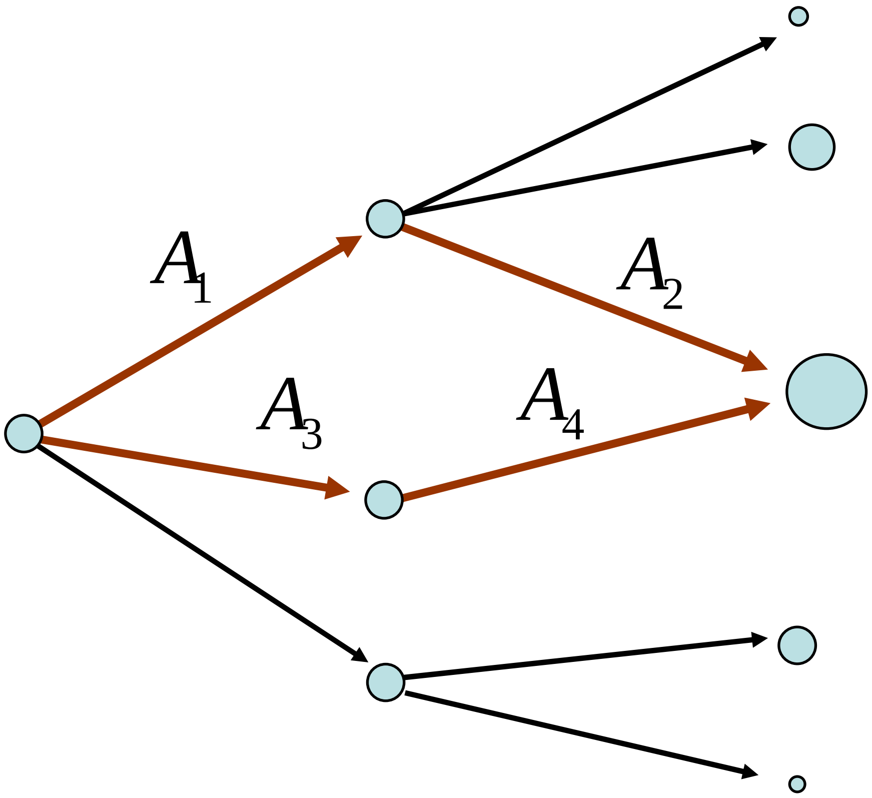


$$P = P_1 P_2 + P_3 P_4$$

input
(a binary string)

possible outputs
(binary strings)

Sequential quantum computation



$$A = A_1 A_2 + A_3 A_4$$

$$P = \left| A_1 A_2 + A_3 A_4 \right|^2$$

$$= \left| A_1 A_2 \right|^2 + \left| A_3 A_4 \right|^2$$

$$+2\,\mathrm{Re}\left(A_1 A_2 A_3^* A_4^* \right)$$

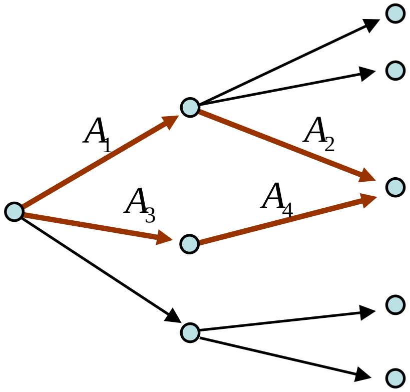
$$\uparrow$$

Constructive interference: enhance correct outputs

Destructive interference: suppress wrong outputs

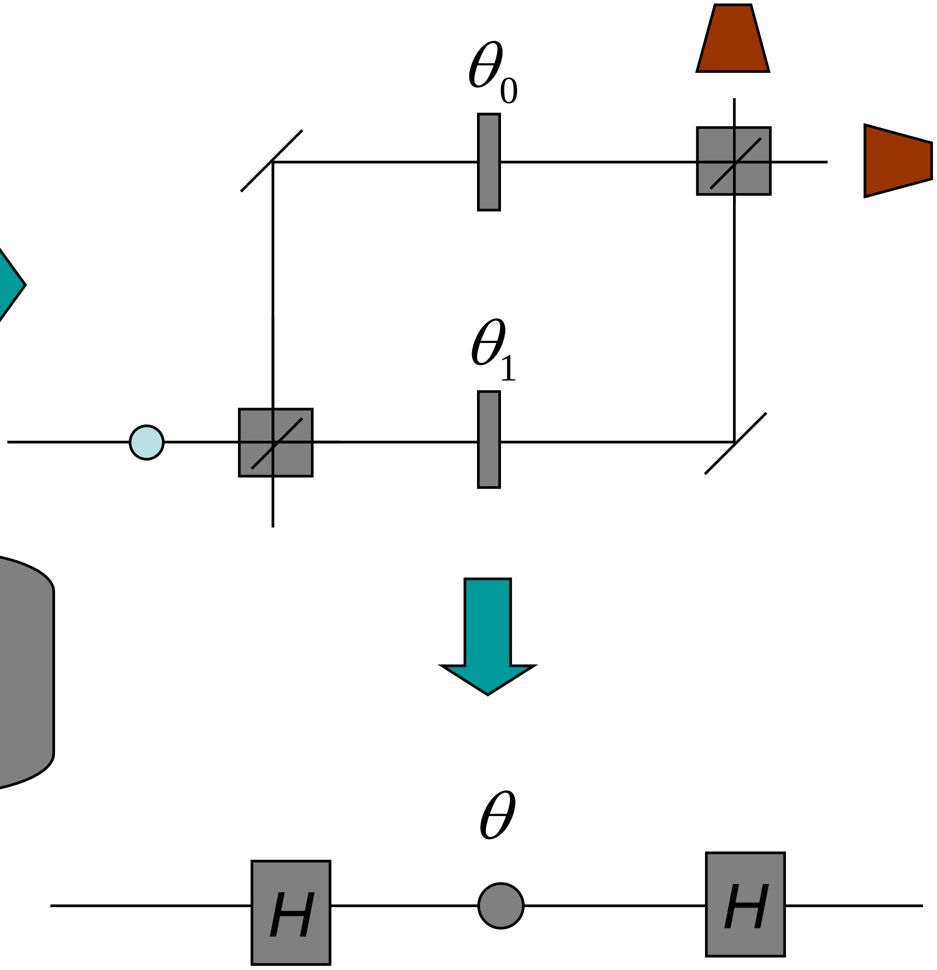
sensitive to decoherence

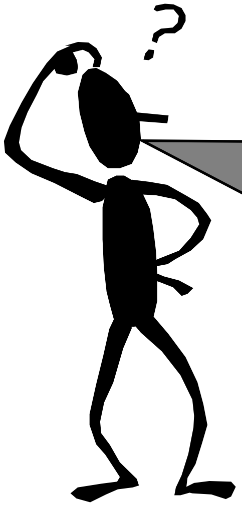
Building quantum computers



$$A = A_1A_2 + A_3A_4$$

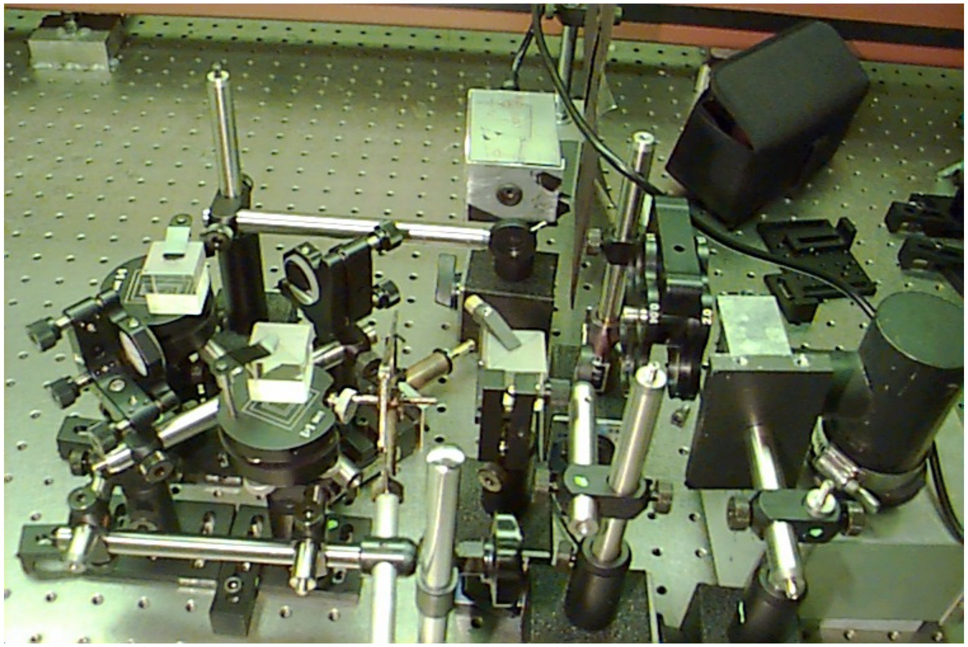
$$P = \left|A_1A_2 + A_3A_4\right|^2$$





In fact, there are many ways of implementing quantum interference…

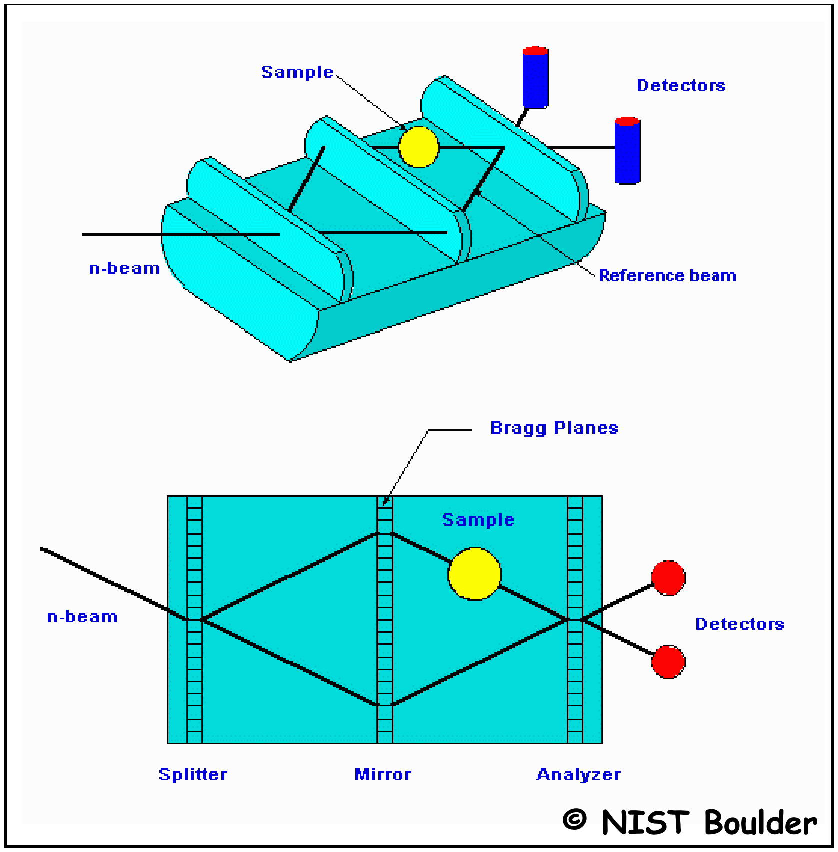
it may looks like this…



© Lauren Hellig

With photons…

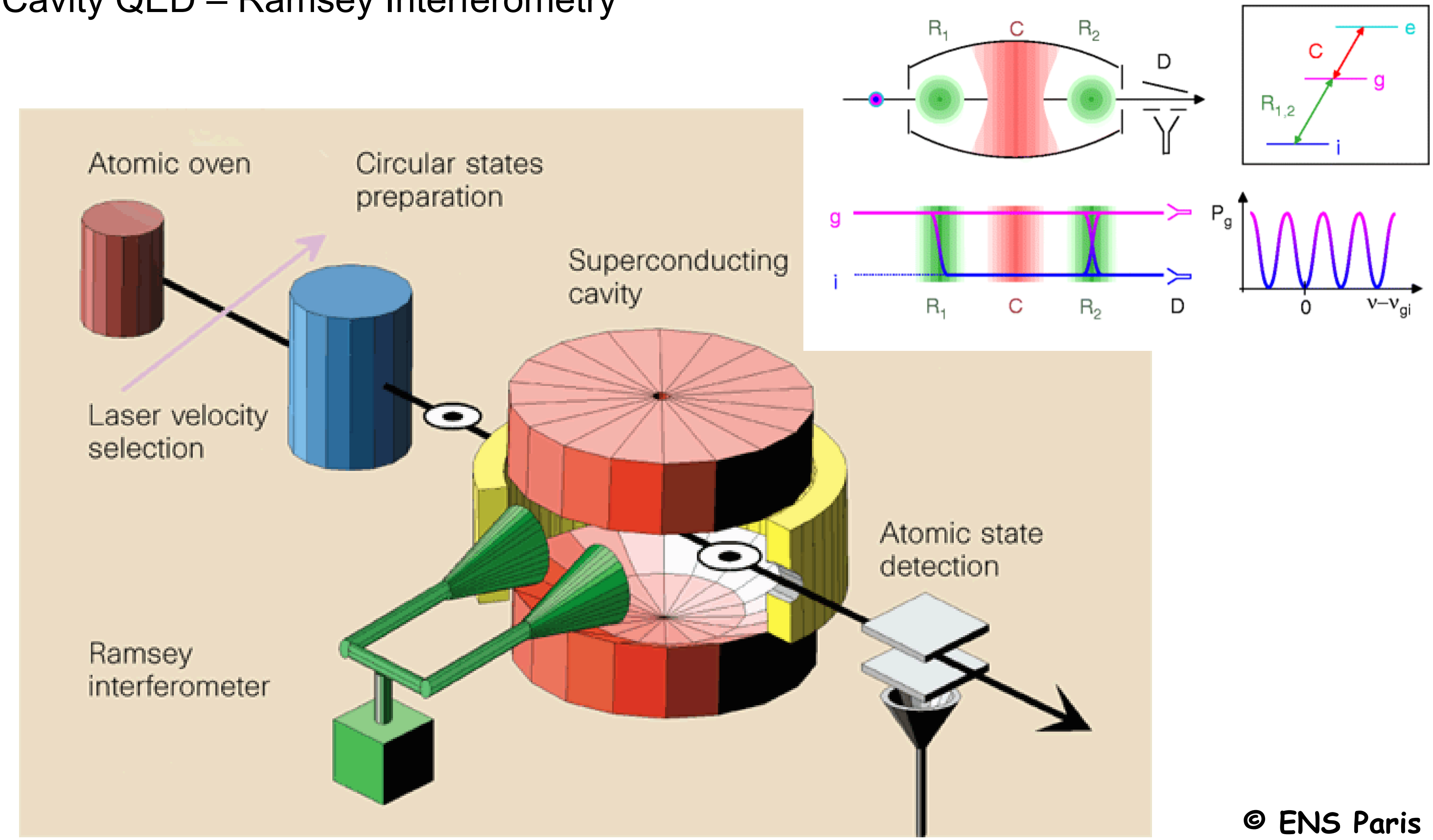
…with neutrons…



© NIST Boulder

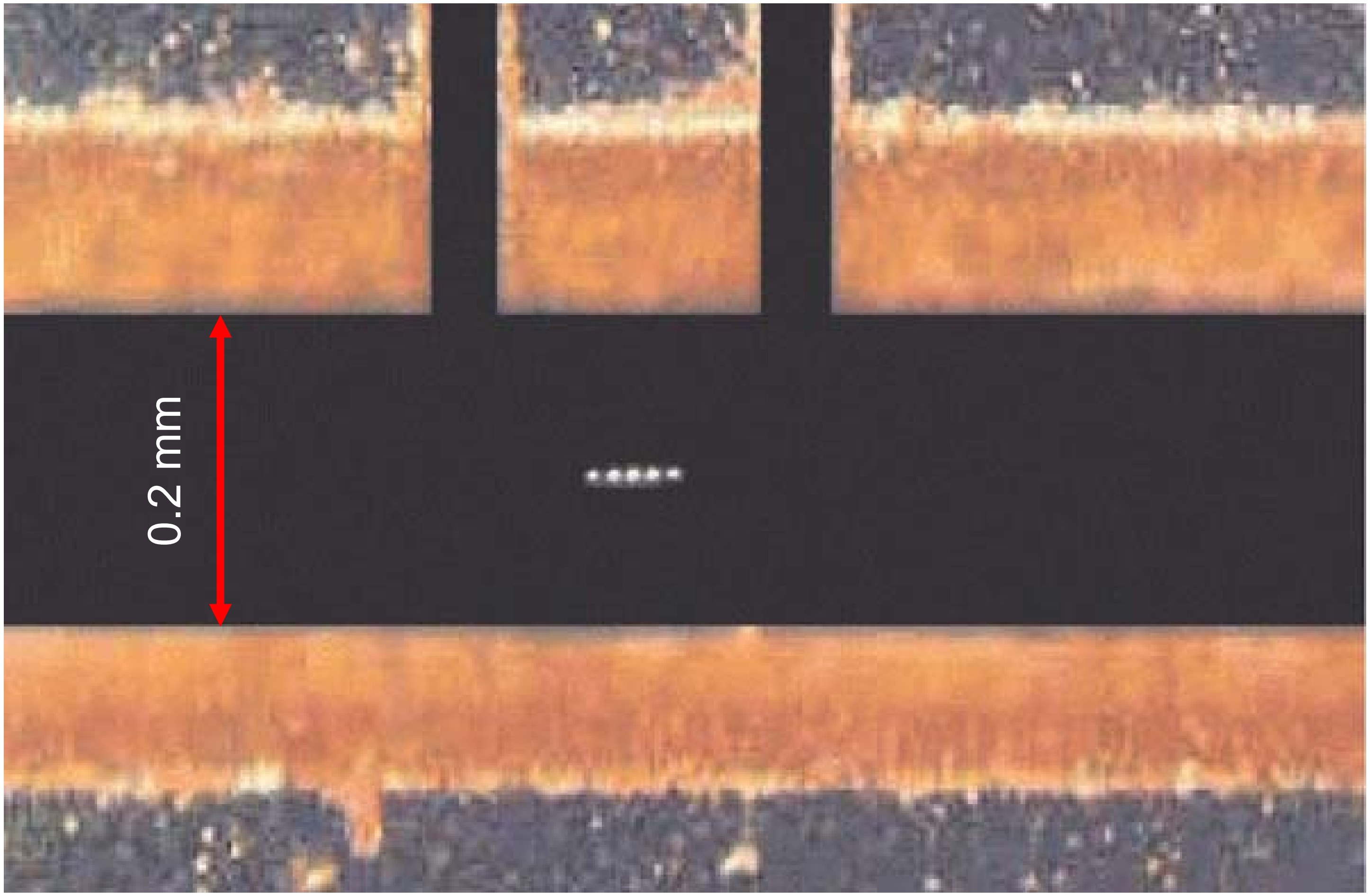
…or like this…

Cavity QED – Ramsey Interferometry



© ENS Paris

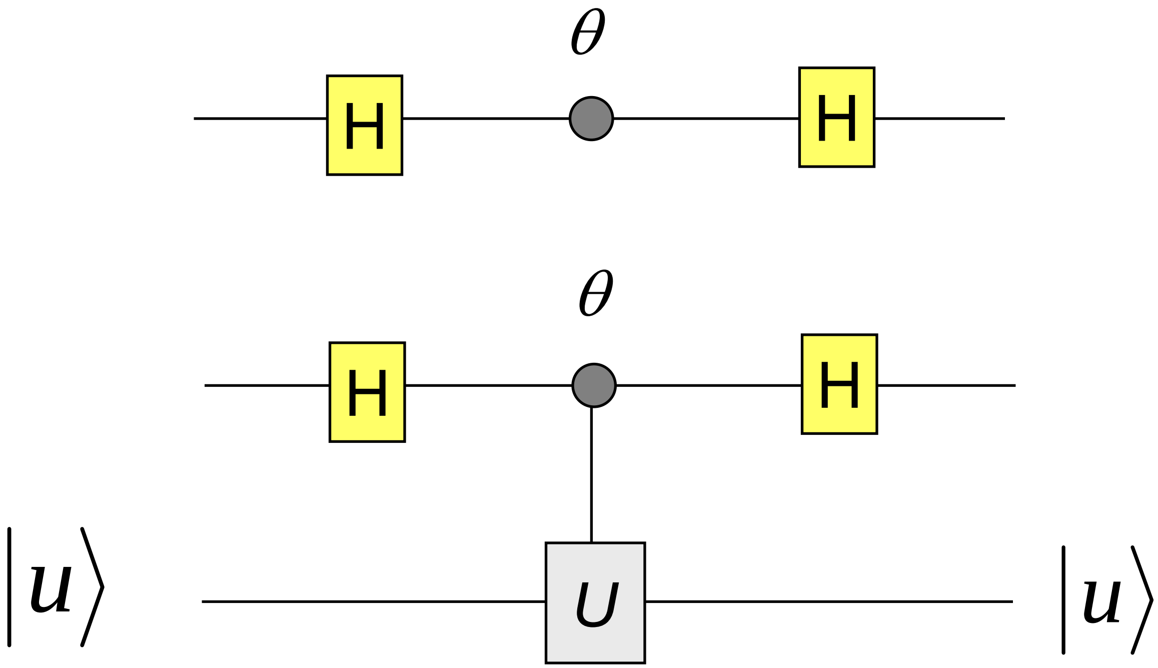
…or like this



Beryllium ions in a trap

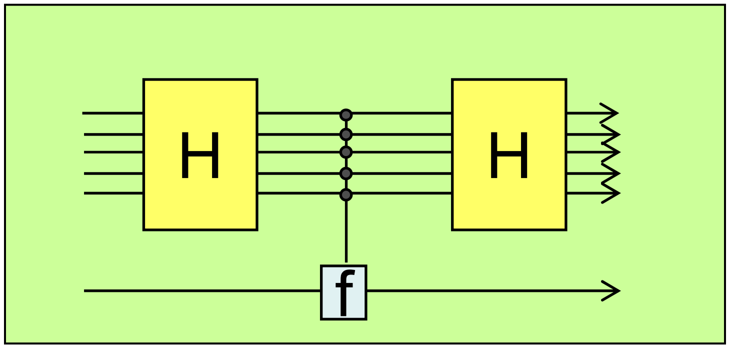
© NIST Boulder

Quantum interferometry revisited

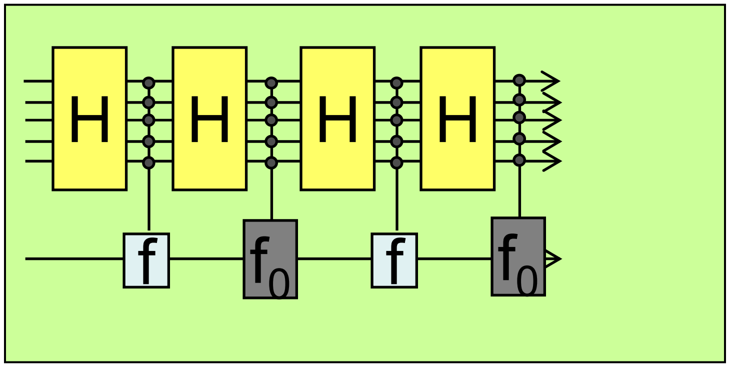


$$U|u\rangle = e^{i\theta}|u\rangle$$

Quantum computation = multiparticle interference



Deutsch (1985), Deutsch and Jozsa (92), Bernstein and Vazirani (92): The first indication that quantum computers can perform better



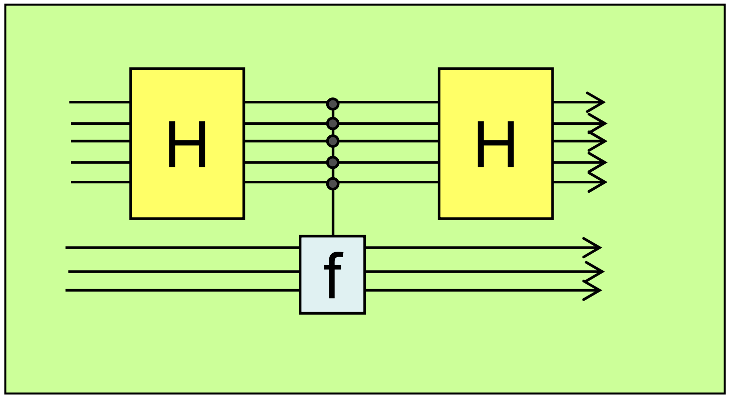
Grover: Polynomial separation

$\Omega\left(2^n\right)$

classical

$O\left(\sqrt{2^n}\right)$

quantum



Simon: Exponential separation

$\Omega\left(\sqrt{2^n}\right)$

classical

$O\left(n\right)$

quantum

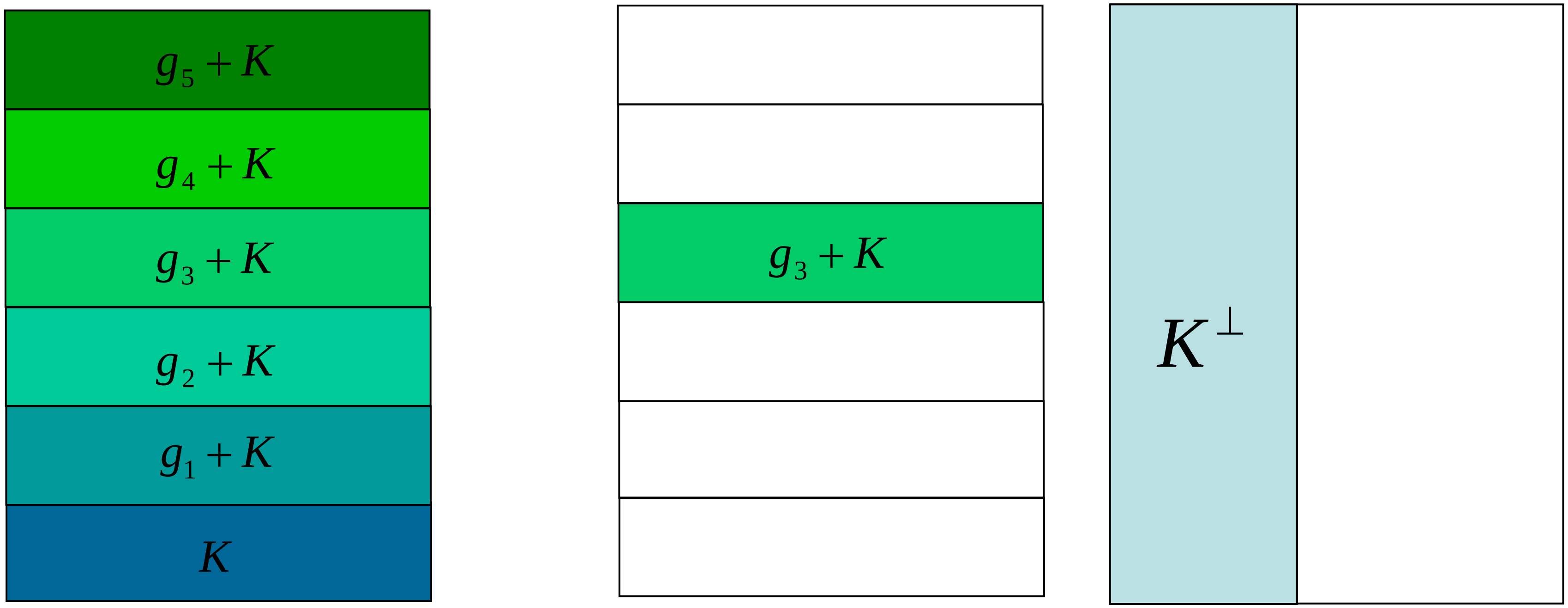
Searching for patters in phases

(hidden subgroups)

Given $f : G \mapsto Y$ constant and distinct o cosets of subgroub K

Find K

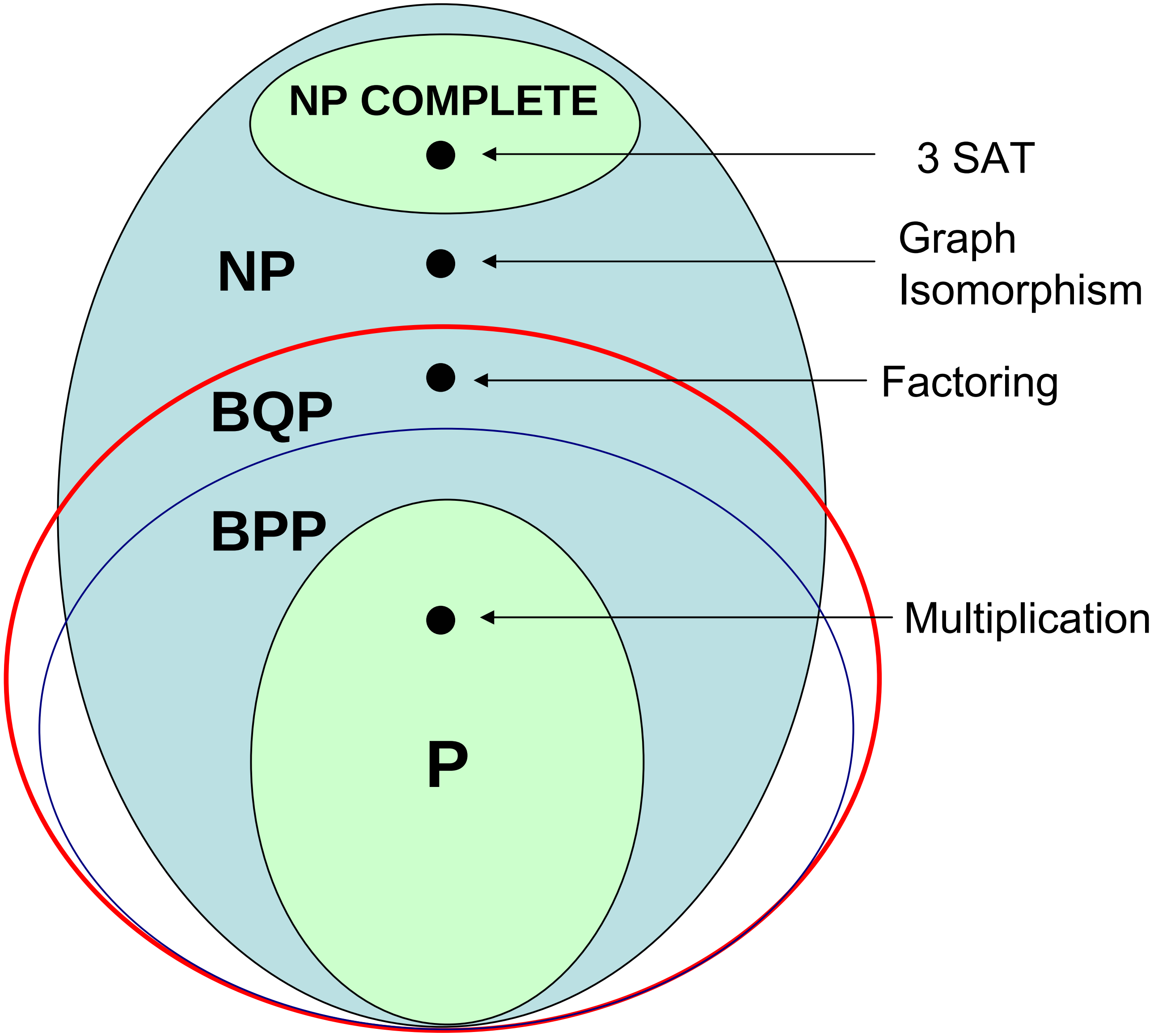
$$|0\rangle|0\rangle \xrightarrow{QFT} \sum_{g\in G}|g\rangle|0\rangle \xrightarrow{f} \sum_{g\in G}|g\rangle|f(g)\rangle \xrightarrow{M} \sum_{k\in K}|g+k\rangle \xrightarrow{QFT} \sum_{k'\in K^{\perp}}|k'\rangle$$



Pushing HSP and QFT to the limits

- Hidden coset problem
    - » e.g. shifted Legendre symbol
- Groups which are not finitely generated
    - » e.g. Pell’s equation
- Difficulties with interesting non-Abelian cases
    - » e.g. symmetric group
- …

Power of quantum computation



Alternative routes

- Adiabatic annealing
- Quantum simulations
- Searching for quantum computation in nature
- …

3-SAT Problem

$$\underbrace{(z_1 \text{ OR } \bar{z}_7 \text{ OR } z_{15})}_{Clause 1} \quad \textbf{AND} \quad \underbrace{(\bar{z}_3 \text{ OR } \bar{z}_8 \text{ OR } z_{11})}_{Clause\ 2} \cdots \quad \textbf{AND} \quad \underbrace{(\bar{z}_i \text{ OR } \bar{z}_j \text{ OR } z_k)}_{Clause\ \text{M}}$$

Energy function

$$h_1 = h(z_1, z_7, z_{15}) = \begin{cases} 0 & \text{if satisfied} \\ 1 & \text{if violated} \end{cases}$$

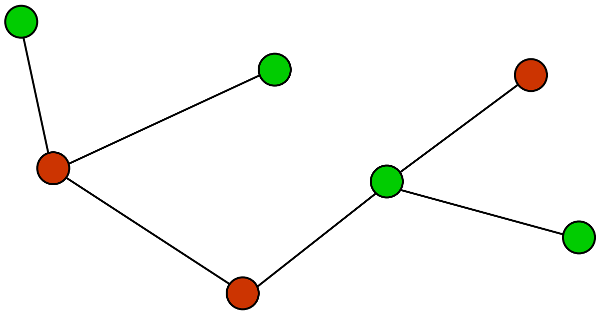
$$h_2 = h(z_3, z_8, z_{11}) = \begin{cases} 0 & \text{if satisfied} \\ 1 & \text{if violated} \end{cases}$$

Search for $z_1, z_2, z_3 \ldots \quad z_n$ that minimize $\boxed{H = \sum_{k=1}^{M} h_k}$

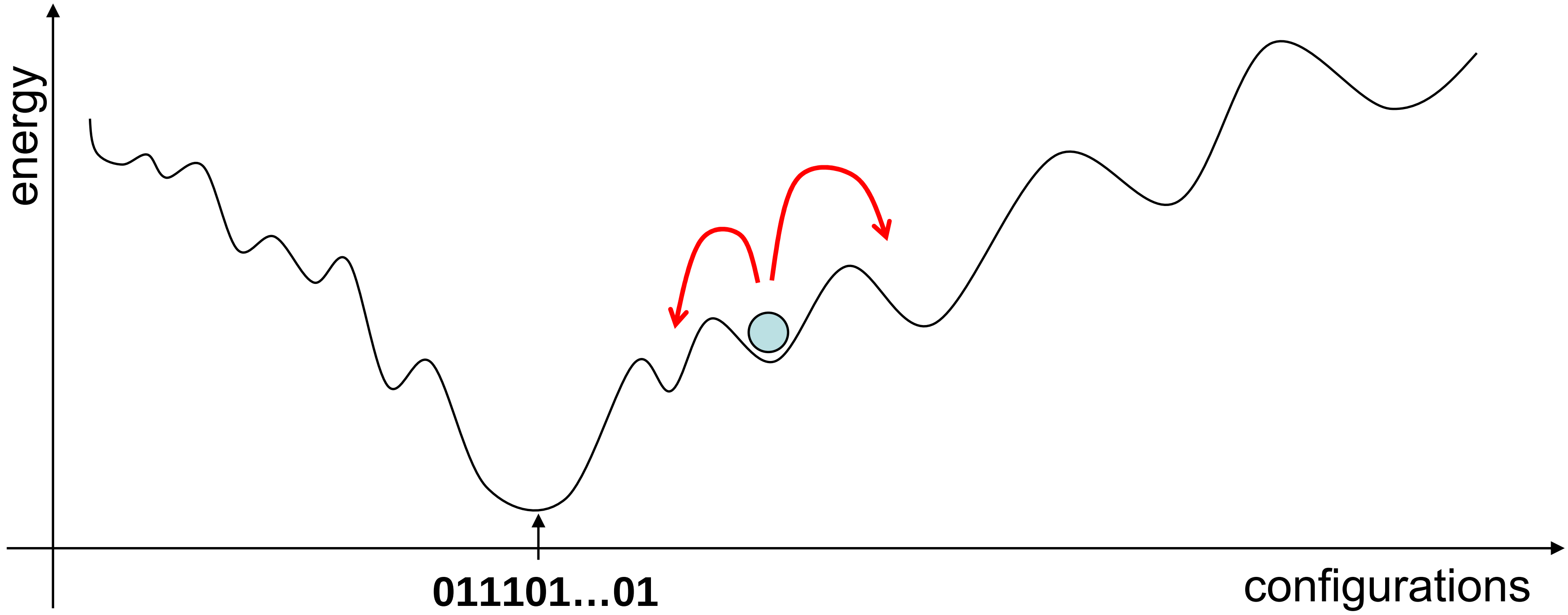
Beyond sequential models

🔴 = 0

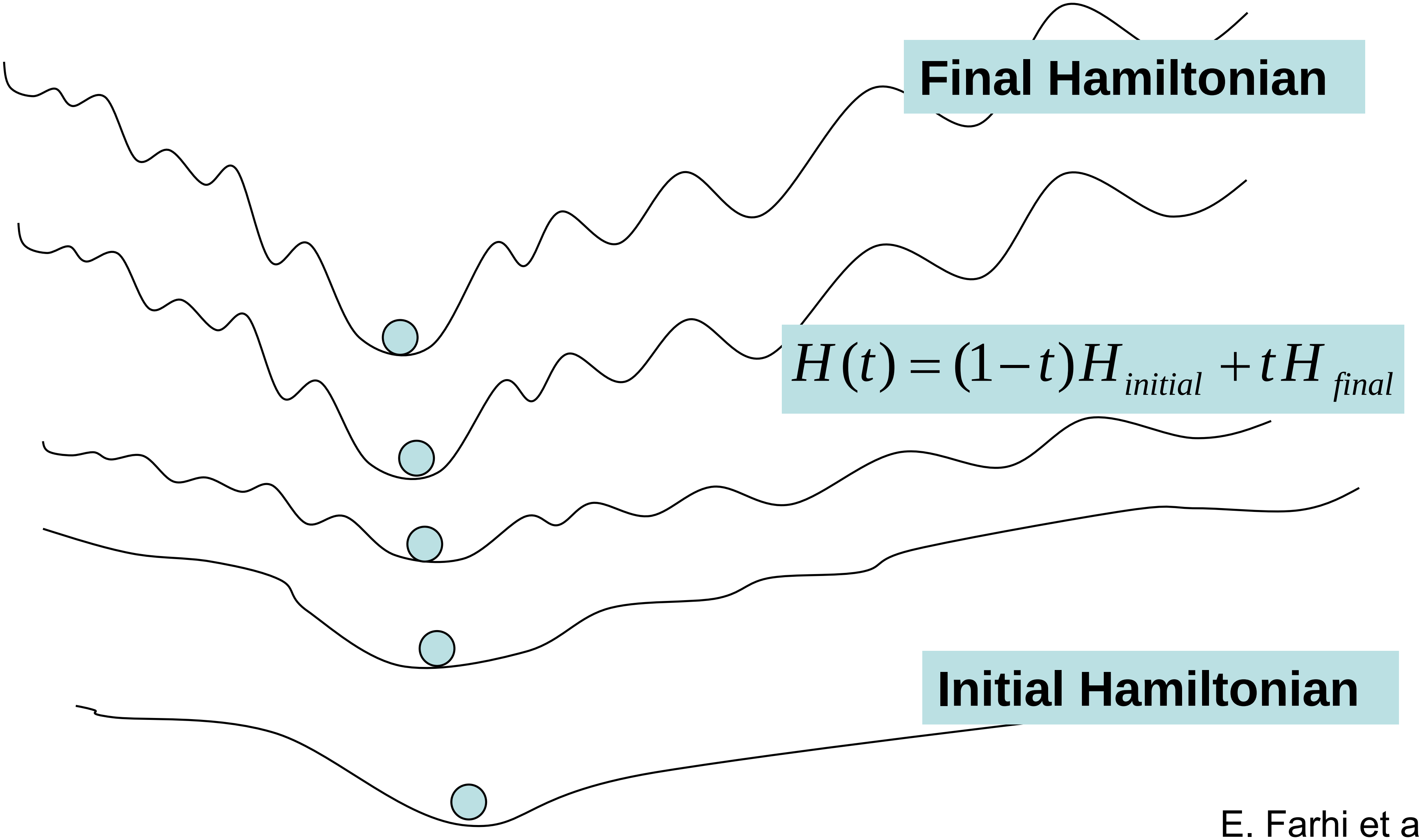
🟢 = 1



searching for the grounds state of interacting spins



Adiabatic Annealing



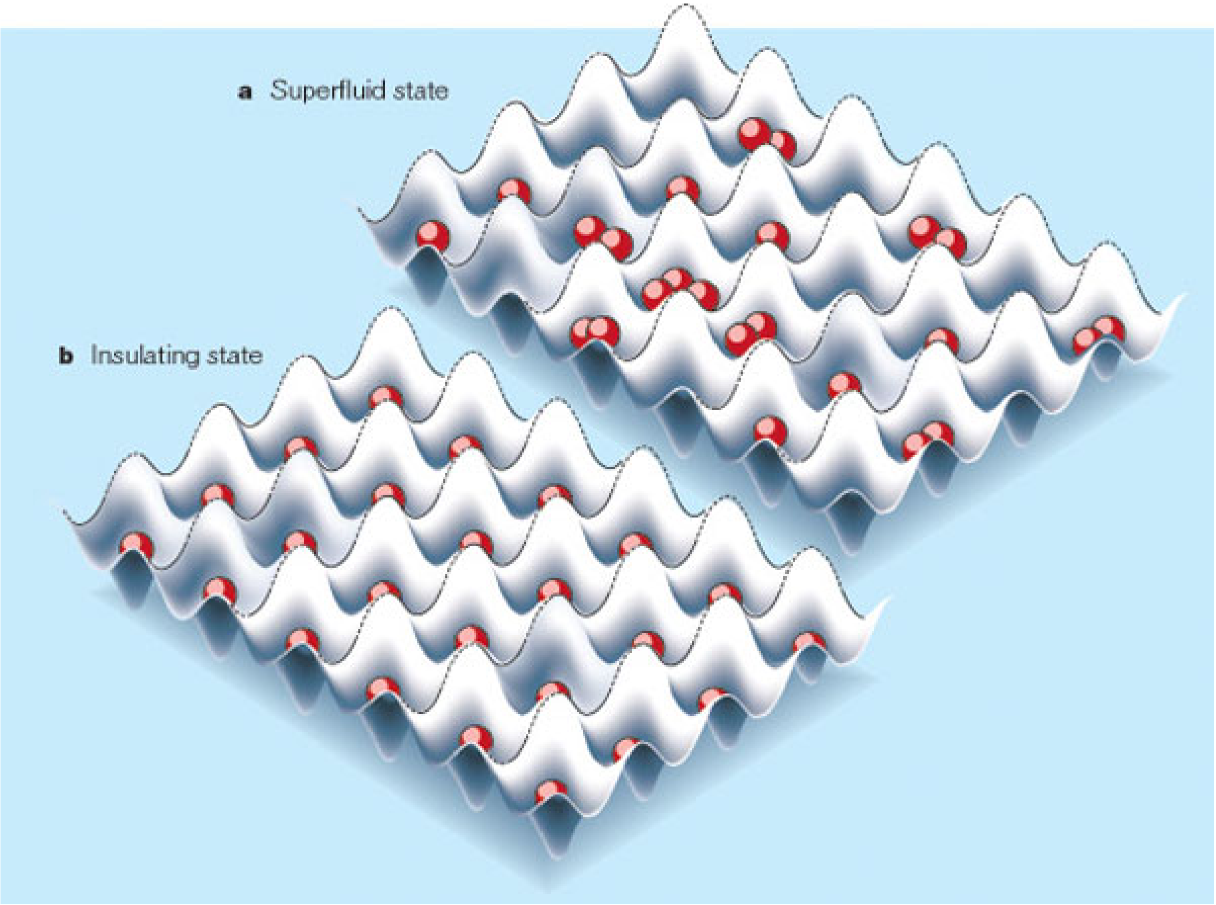
Final Hamiltonian

$$H(t) = (1-t)H_{initial} + tH_{final}$$

Initial Hamiltonian

E. Farhi et al

Simulation of quantum phase transitions



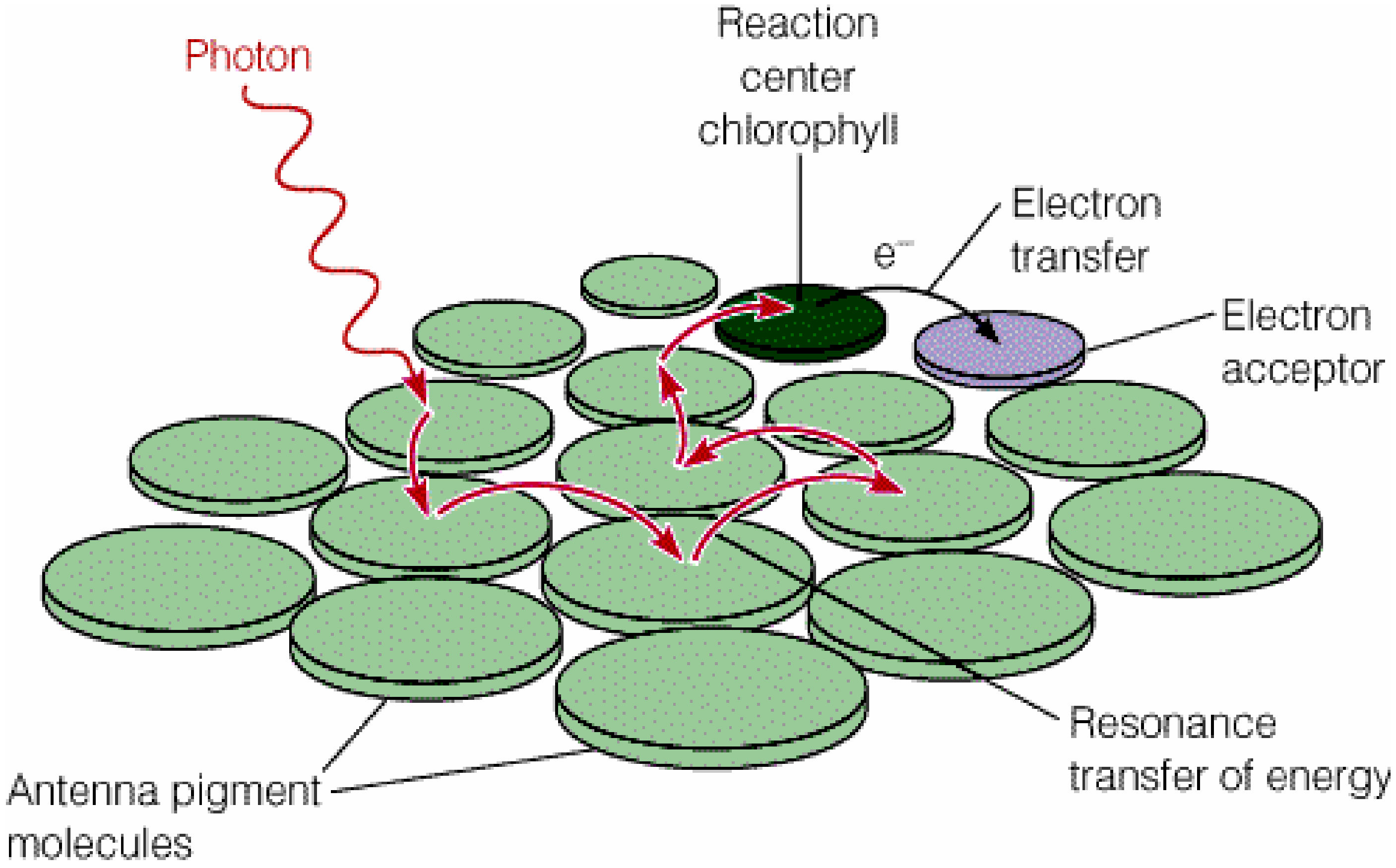
Quantum simulations

Tool for investigating properties of many body systems and exotic materials

Reversible switch between a superfluid and an insulating phase of a gas of rubidium atoms in optical lattices

M. Greiner et al., Nature 415, 39 (2002)

Coherent quantum phenomena in nature ?

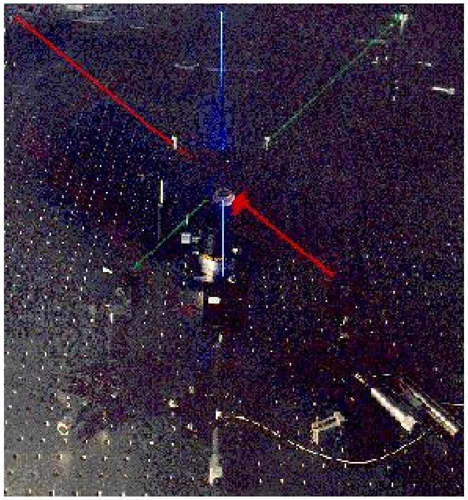


Power of quantum physics

The quantum taketh away… …and the quantum giveth back!

~~RSA Data Security.~~
~~A Security Dynamics Company~~

Quantum factoring and discrete log (Shor 94)
Quantum search (Grover 96)
Solving Pell's equation (Hallgren 02)
Dihedral HSP (Kuperberg 03)



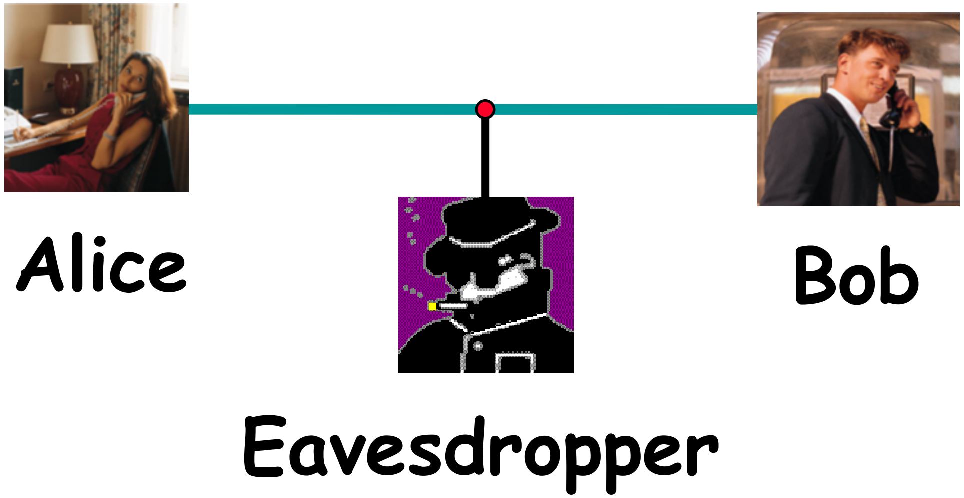
Quantum cryptography

© DRA Malvern (1990)

Two cryptographic scenarios

Secret Key Distribution

Alice and Bob trust each other but must face a common enemy - an eavesdropper Eve



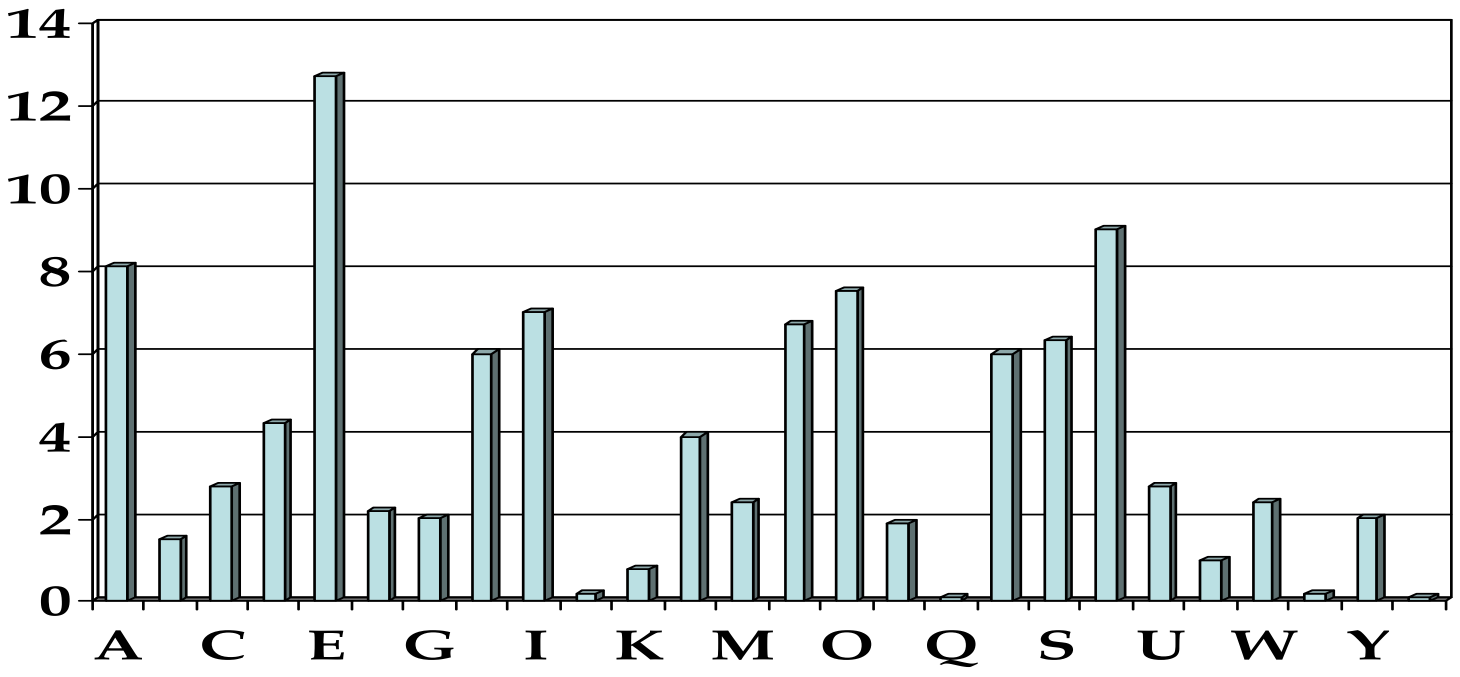
Mistrustful Cryptography

Alice and Bob do not have big enemies but they do not trust each other

Early cryptanalysis

Baghdad, al-Kindi (800-873

Frequency analysis



Frequency of letters in a typical English text

Counterexamples - Lipograms

That's right - this is a lipogram - a book, paragraph or similar thing in writing that fails to contain a symbol, particularly that symbol fifth in rank out of 26 (amidst 'd' and 'f') and which stands for a vocalic sound such as that in 'kiwi'. I won't bring it up right now, to avoid spoiling it…

First lipogram: Lasus of Achaia (600 BC)

The most famous lipogram:

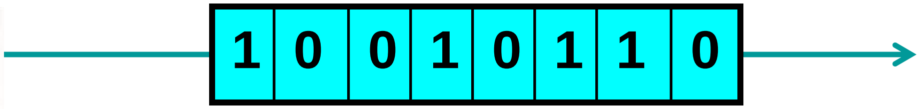
Georges Perec, *La Disparition* (1969)
85 000 words without the letter e

English translator, Gilbert Adair, in *A Void*, succeeded in avoiding the letter e as well

Tout avait l'air normal, mais tout s'affirmait faux. Tout avait l'air normal, d'abord, puis surgissait l'inhumain, l'affolant. Il aurait voulu savoir où s'articulait l'association qui l'unissait au roman : sur son tapis, assaillant à tout instant son imagination, …

One-time pad

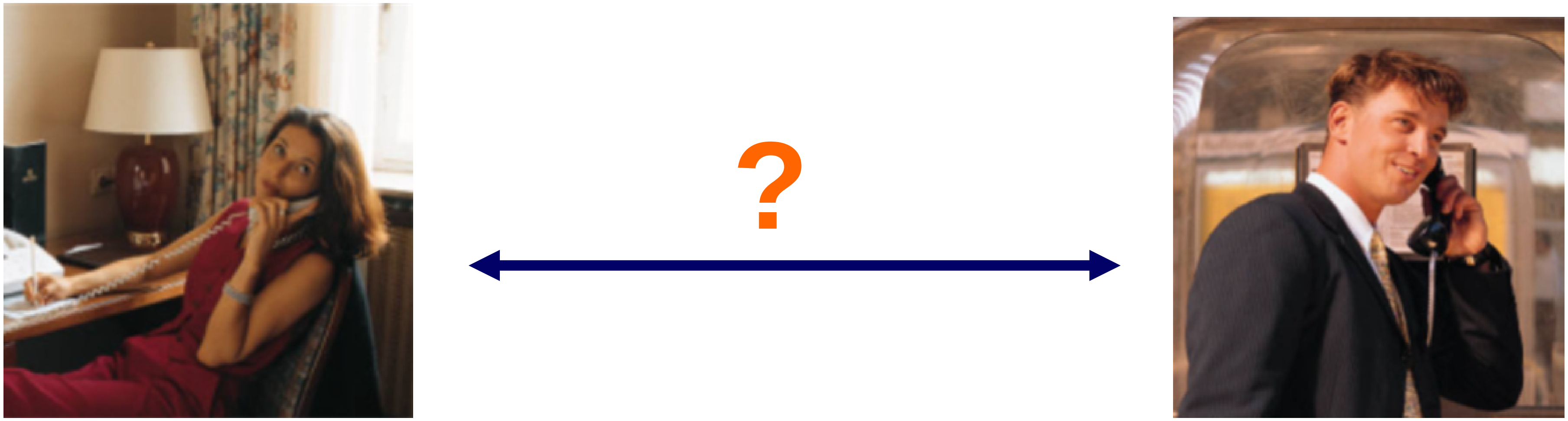
01011100	plaintext
11001010	KEY
10010110	cryptogram



1	0	0	1	0	1	1	0

cryptogram	10010110
KEY	11001010
plaintext	01011100

Key distribution problem



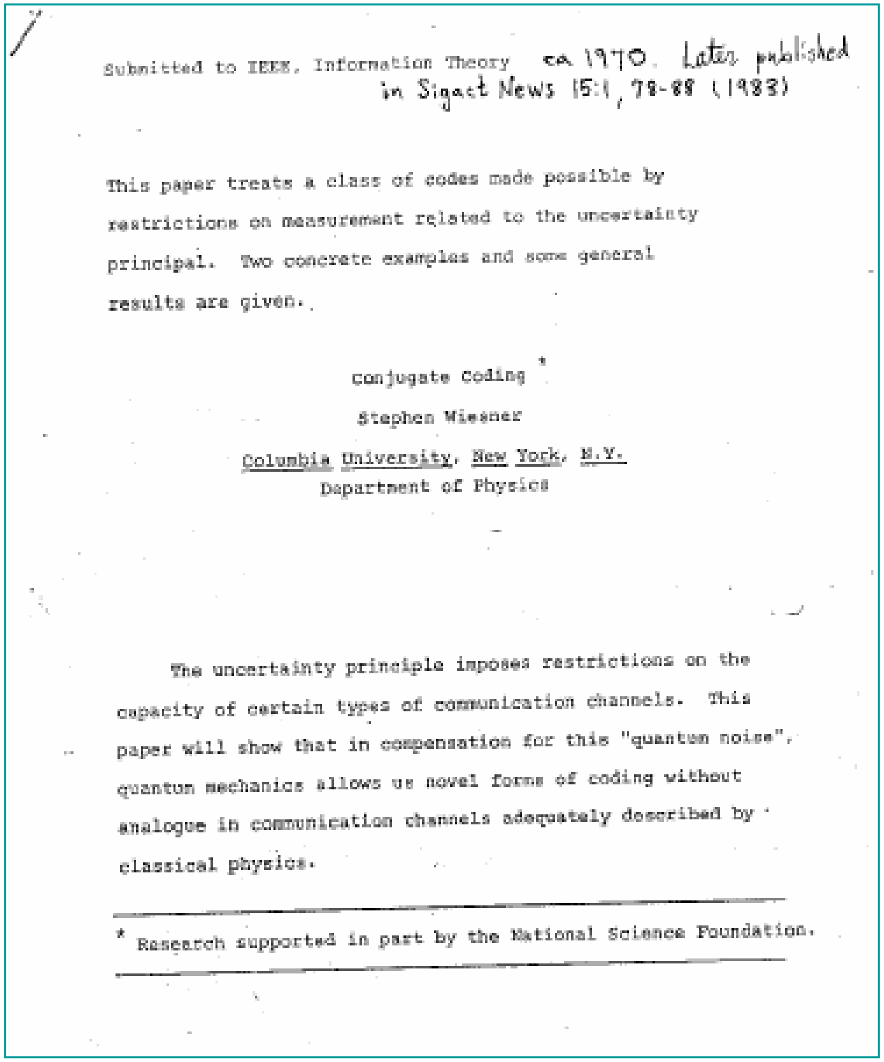
KEY	0	0	1	0	1	1	0

KEY	0	0	1	0	1	1	0

Possible solutions

- **Public key cryptosystems**
  - **mathematical, security based on computational complexity**
  - Can be broken by quantum computers!
- **Quantum cryptography**
  - Physical, security based on
    - **Quantum entanglement (A. Ekert)**
    - **Heisenberg's Uncertainty Principle (S. Wiesner)**

Origins of quantum cryptography



Submitted to IEEE, Information Theory ca 1970. Later published in Sigact News 15:1, 78-88 (1983)

This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

conjugate coding*

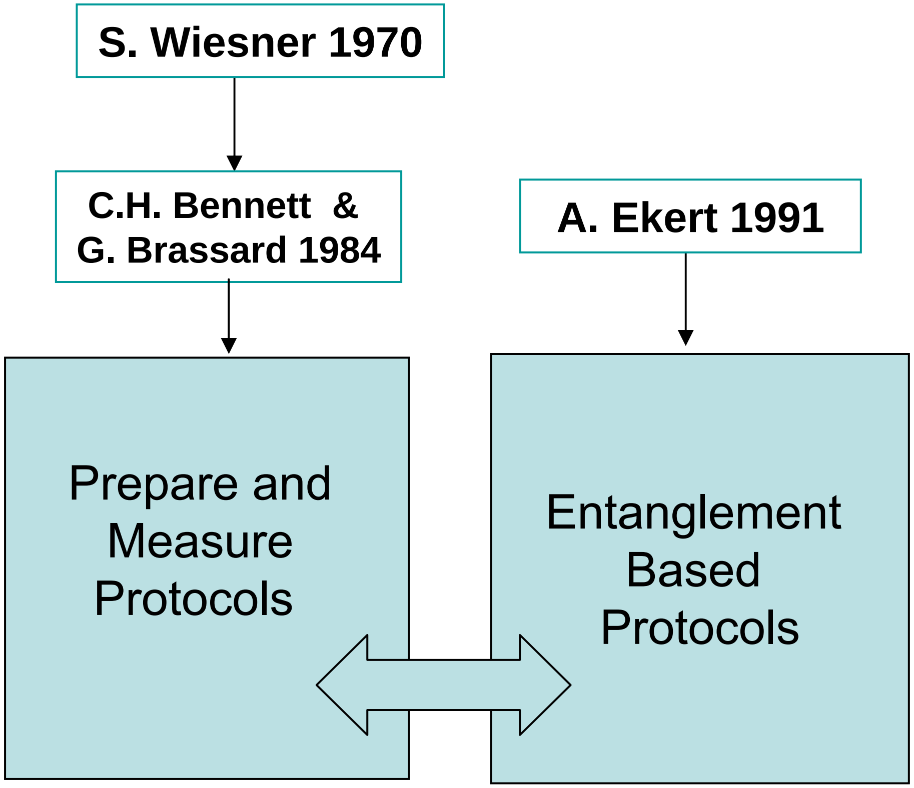
Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

---

* Research supported in part by the National Science Foundation.



S. Wiesner 1970

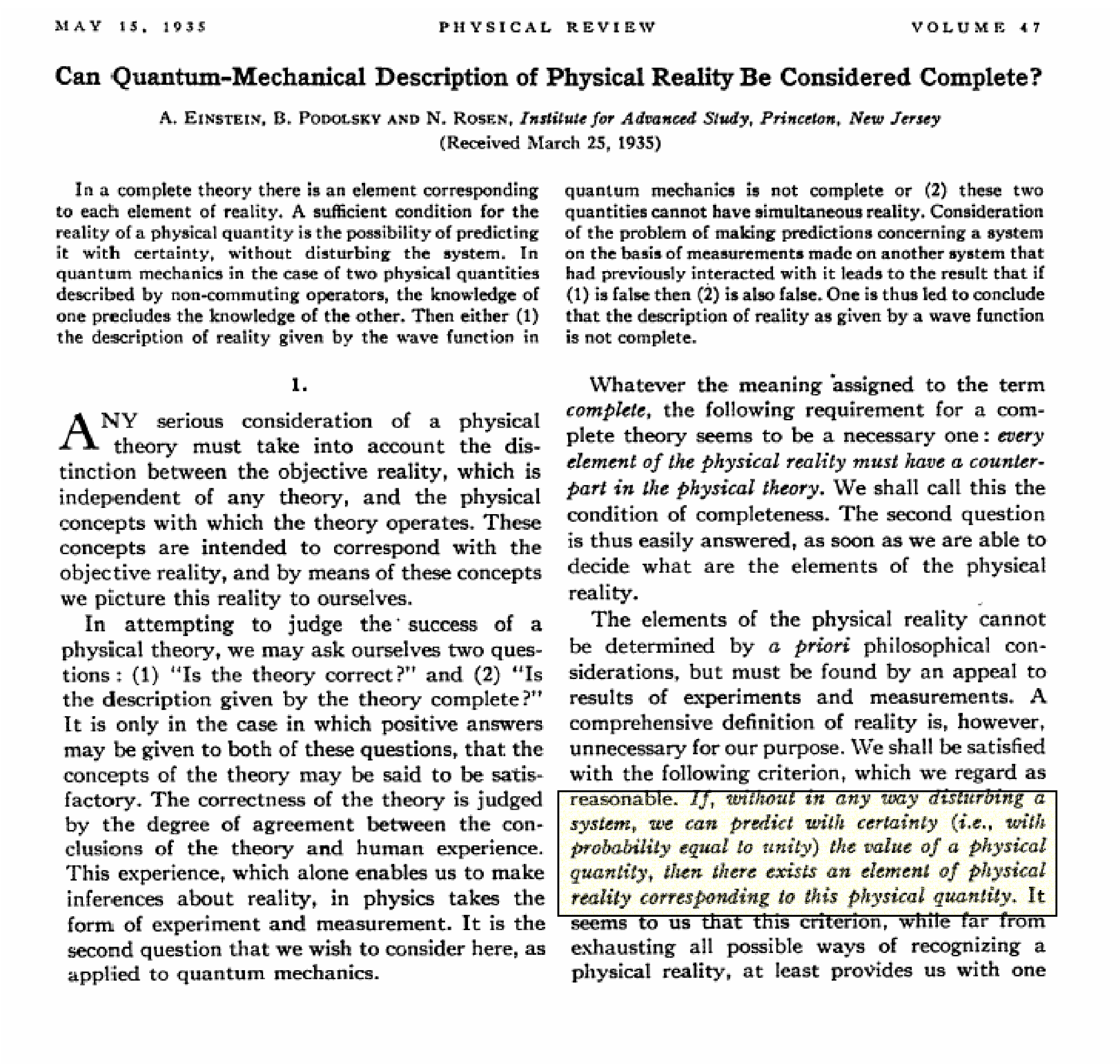
C.H. Bennett & G. Brassard 1984

A. Ekert 1991

Prepare and Measure Protocols

Entanglement Based Protocols

But it could have been invented in 1935



MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. Einstein, B. Podolsky and N. Rosen, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

Any serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

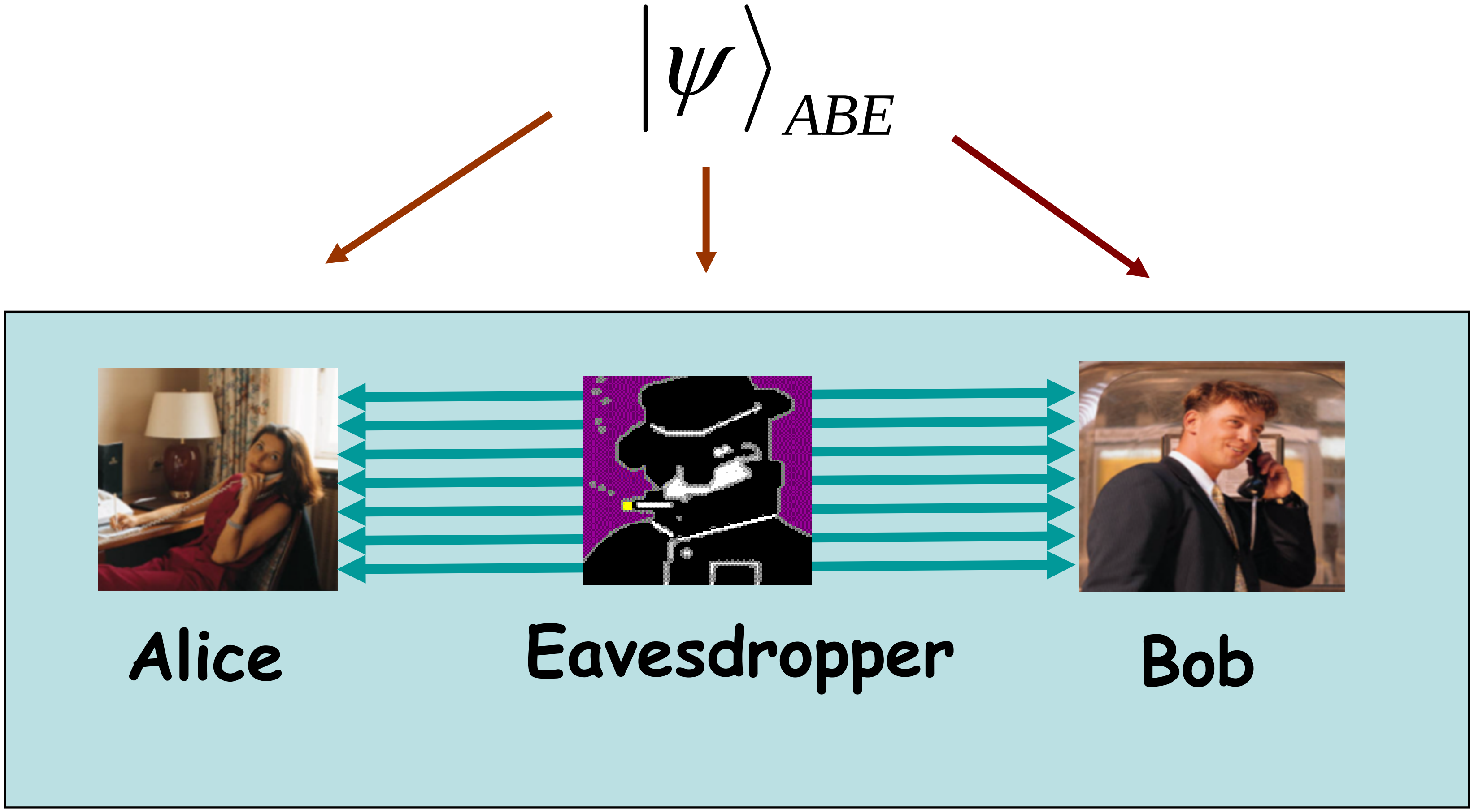
Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory.* We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

–"If, without in any way disturbing a system, we can predict with certainty… the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity"

PERFECT EAVESDROPPING

Eavesdropper distributes the key



$$|\psi\rangle_{ABE}$$

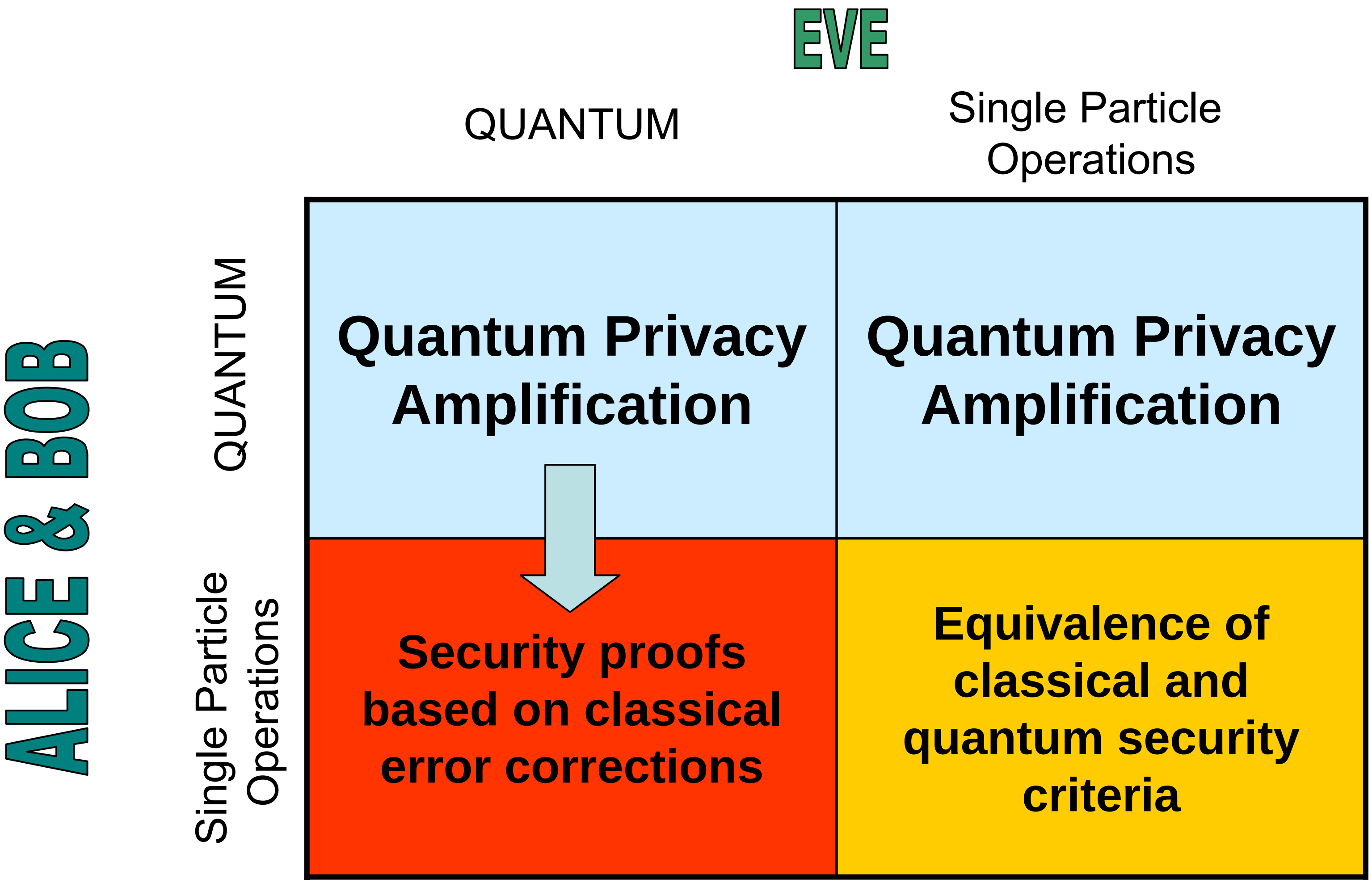
Alice

Eavesdropper

Bob

Eavesdropping scenarios

		EVE	
		QUANTUM	Single Particle Operations
ALICE & BOB	QUANTUM	**Both sides have access to quantum technology**	All power to Alice & Bob (not very challenging)
	Single Particle Operations	**All power to Eve**	Interesting connections with Bell Theorems and Advantage Distillation Protocols



EVE

ALICE & BOB

	QUANTUM	Single Particle Operations
QUANTUM	**Quantum Privacy Amplification**	**Quantum Privacy Amplification**
Single Particle Operations	**Security proofs based on classical error corrections**	**Equivalence of classical and quantum security criteria**

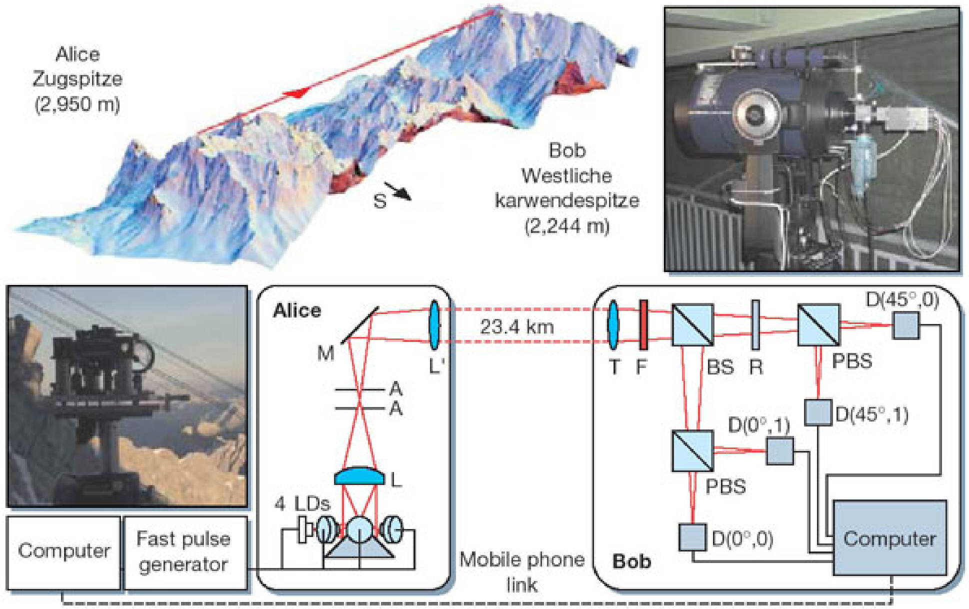
D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *PRL* **77**(13), 2818 (1996).

D. Mayers, Science 283, 2050–2056 (1999) Journal of the ACM 48(3), 351–406 (2001), (quant-ph/9802025)

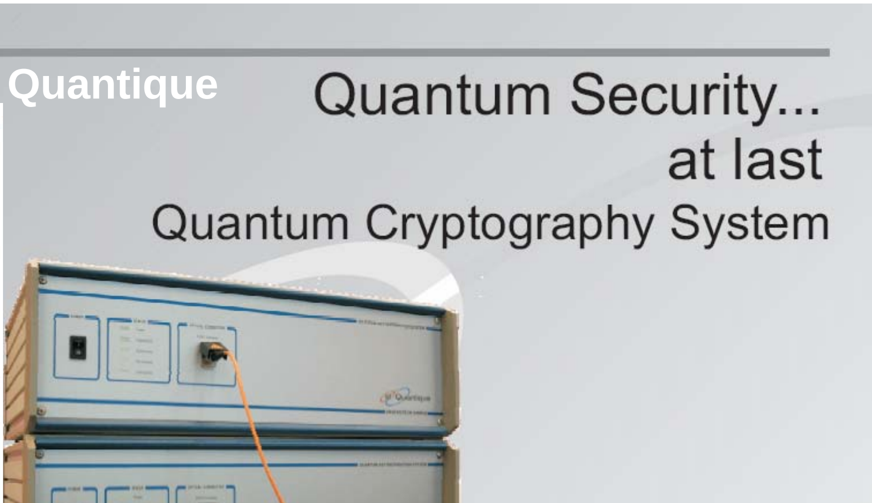
H.-K. Lo and H. F. Chau, Science 283, 2050–2056 (1999)

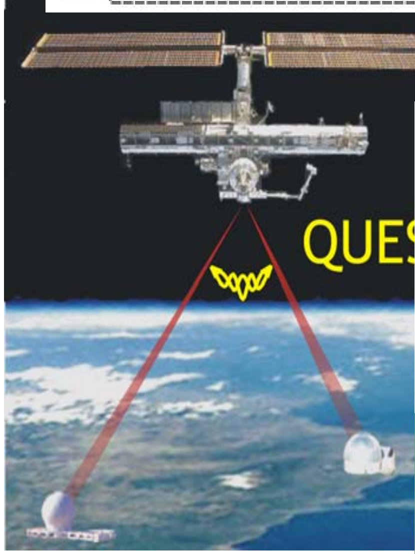
P. Shor and J. Preskill PRL 85, 411 (2000)

Today…

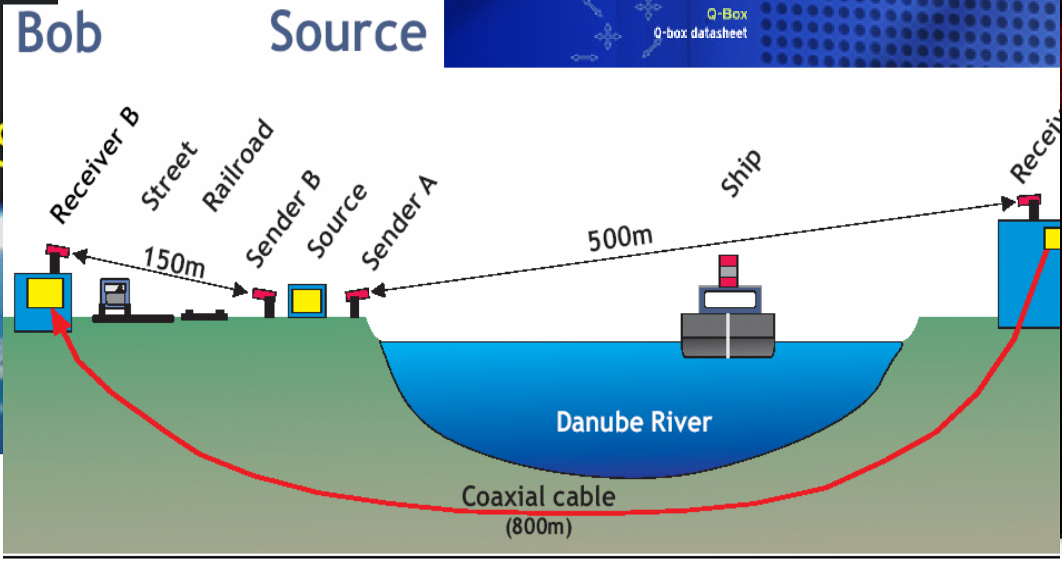


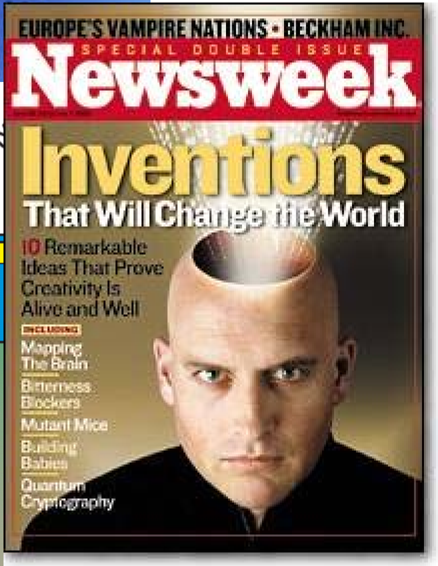
C. Kurtsiefer et al.





A. Zeilinger et al.





Mistrustful cryptography

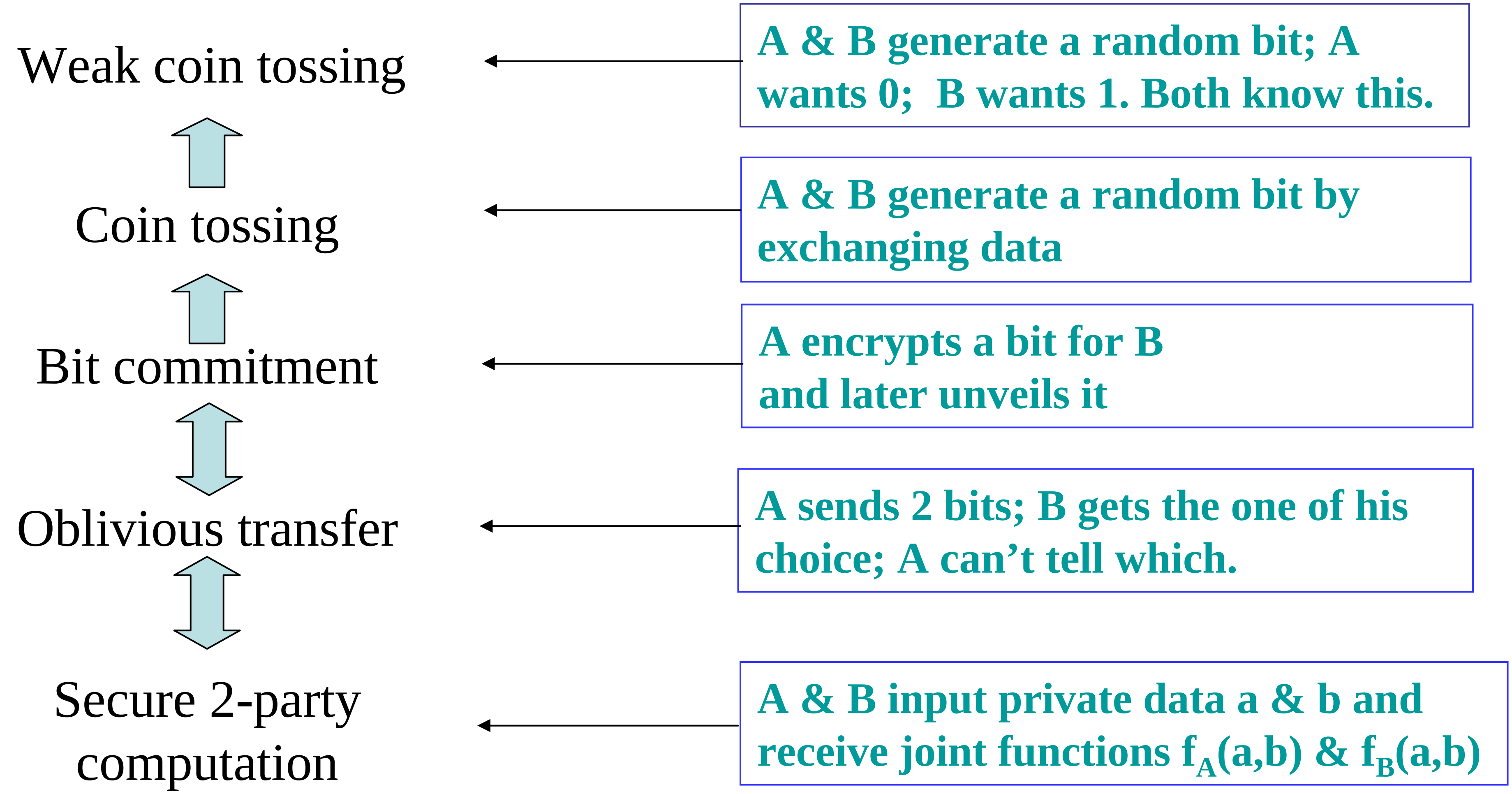
Alice

Controlled information exchange between not necessarily trusting parties.

Bob

Examples: trustable electoral systems that allow secret ballot, secure auctions, tax collection that preserves privacy, remote authentication to a computer, decisions on joint corporate (or other) ventures, job interviews, “helping the police with their enquiries”, …

Hierarchy of primitives



Weak coin tossing

Coin tossing

Bit commitment

Oblivious transfer

Secure 2-party computation

A & B generate a random bit; A wants 0; B wants 1. Both know this.

A & B generate a random bit by exchanging data

A encrypts a bit for B and later unveils it

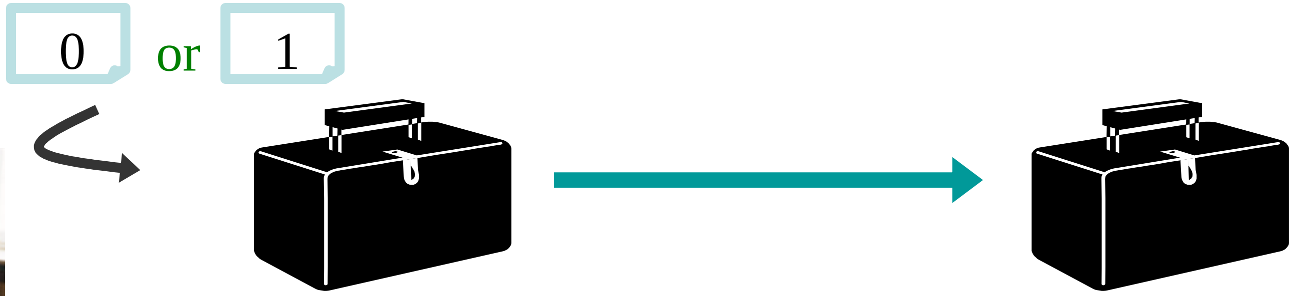
A sends 2 bits; B gets the one of his choice; A can't tell which.

A & B input private data a & b and receive joint functions $f_A(a,b)$ & $f_B(a,b)$

$X \longrightarrow Y$ Y can be securely implemented by a secure black box implementing X, and classical information exchanges

What is bit commitment?

1. Commit Phase:

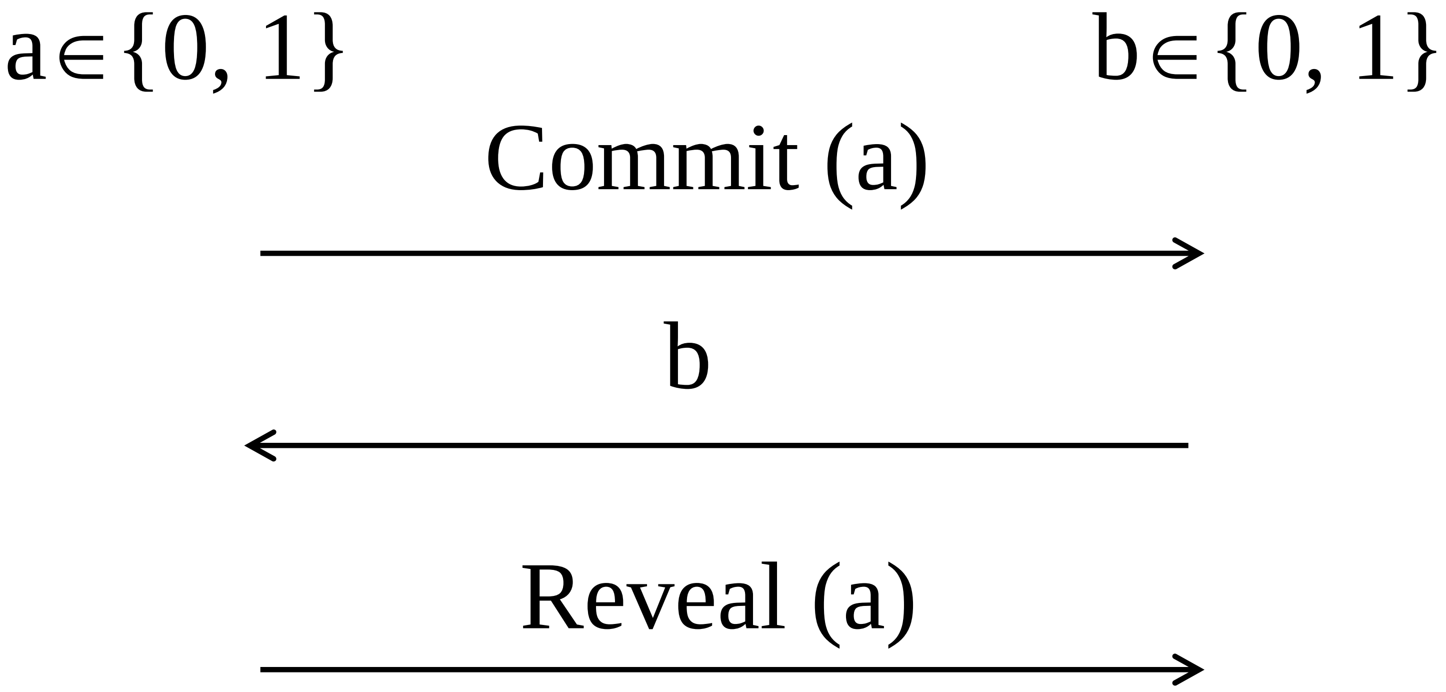


Bob

2. Opening Phase:

Alice can prove to Bob that she has made up her mind during the commit phase and she cannot change it. Yet, Bob does not know her choice until the opening phase.

Bit Commitment Implies Coin Tossing



$a \in \{0, 1\}$

$b \in \{0, 1\}$

Commit (a)

b

Reveal (a)

Result: (a+b) mod 2.

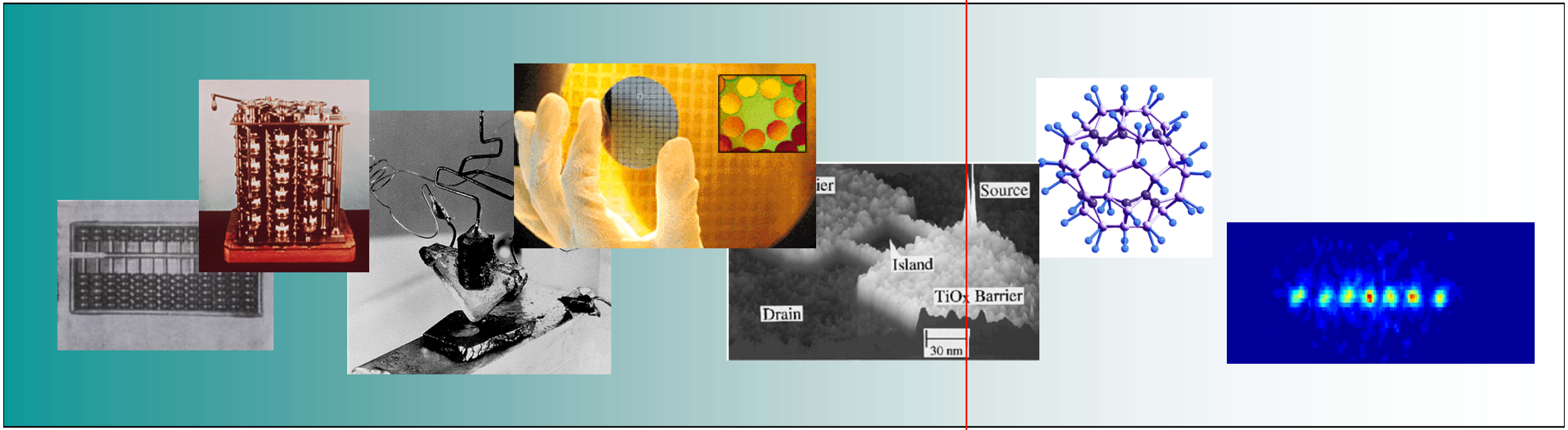
Interesting results and directions

- **Quantum bit commitment**
  - Employ relativity (Kent)
  - Quantum-computational security (Dumais et al. & Cleve et al.)

- **Coin tossing**
  - Strong version: protocol ¾ (Ambainis), lower bound 1/√2 (Kitaev)
  - Weak version: protocol 1/√2 (Rudolph & Spekkens), lower bound >0

- **OPEN PROBLEMS**
  - Better coin tossing protocols/bounds
    - Protocols which are not based on bit commitment (Salvail)
    - Multiple use of bit commitment 9/16 (Nayak & Shor)
    - Coin flipping with penalty for cheating. Trade-offs
  - …
- Many other interesting topics
  - Digital signatures
  - Authentication
  - Fingerprinting
  - …

What is it good for ?



Year 1850 - Michael Faraday in reply to a question by William Gladstone, then British minister of finance (Chancellor of the Exchequer) if electricity had any practical value:

"One day, sir, you may tax it"