AN INVITATION TO

QUANTUM INFORMATION AND CONTROL

Francesco Ticozzi

Deptartment of Information Engineering, University of Padova

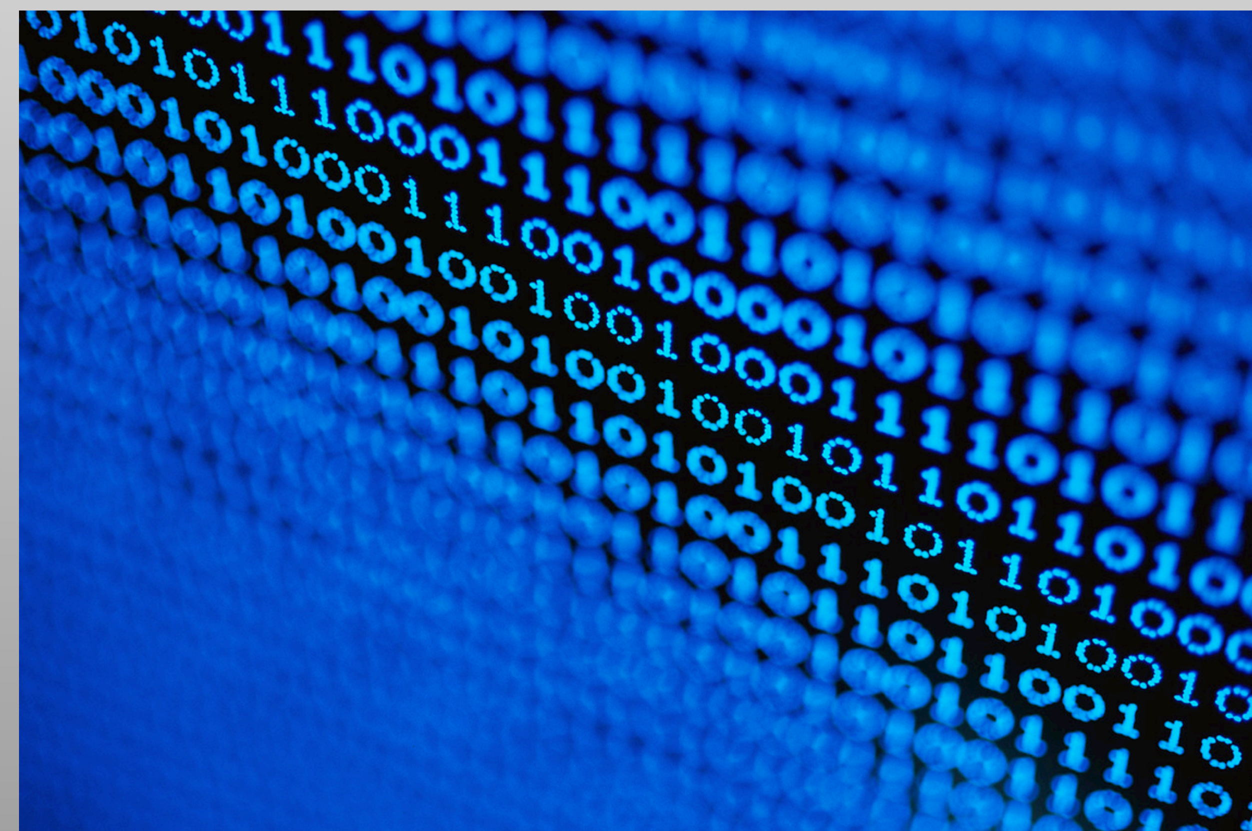
ticozzi@dei.unipd.it

In principle was the Bit...

- Basic unit of (classical) information:

  1 Bit: Choice over two alternatives, in binary labelled as 0, 1

Well-known building block
of the digital revolution...

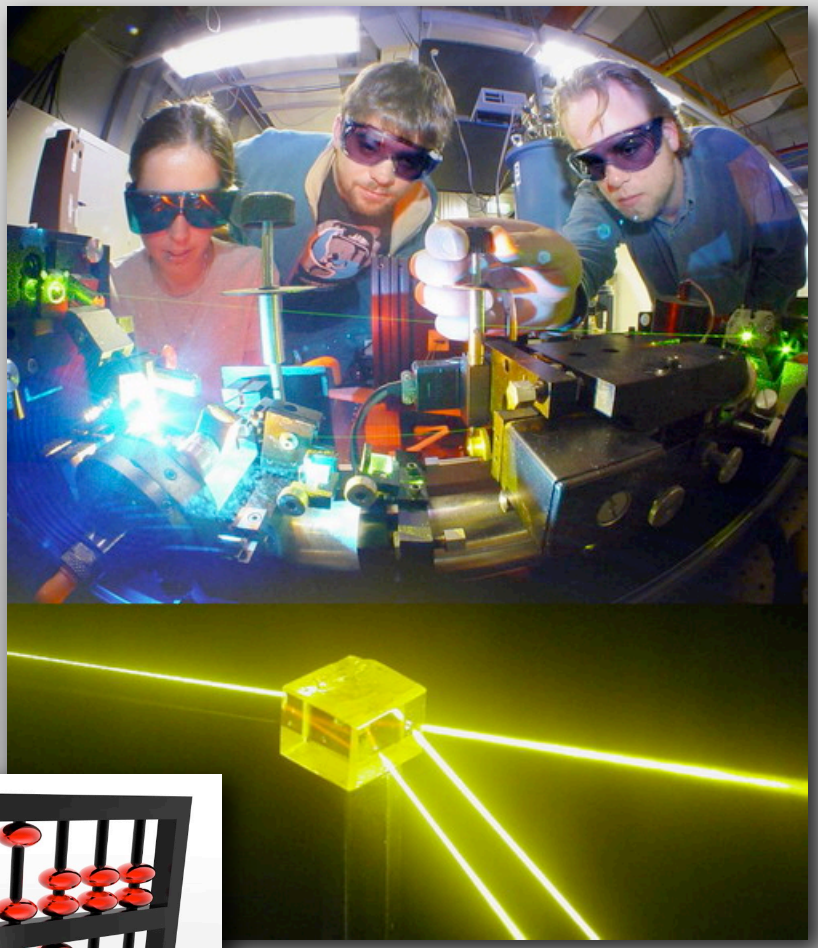


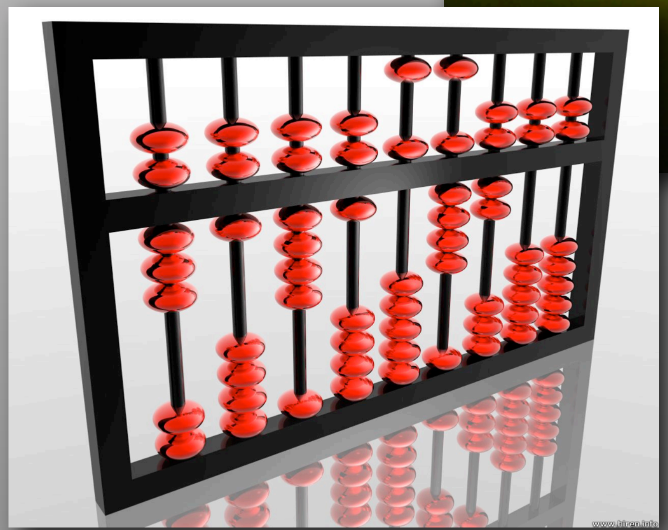
What is information?

- Information regards a *choice over some alternatives*;
- **What these alternatives represent is irrelevant** from an information-theoretic viewpoint;

However, it turns out that...

- **What I encode my information on is relevant...**

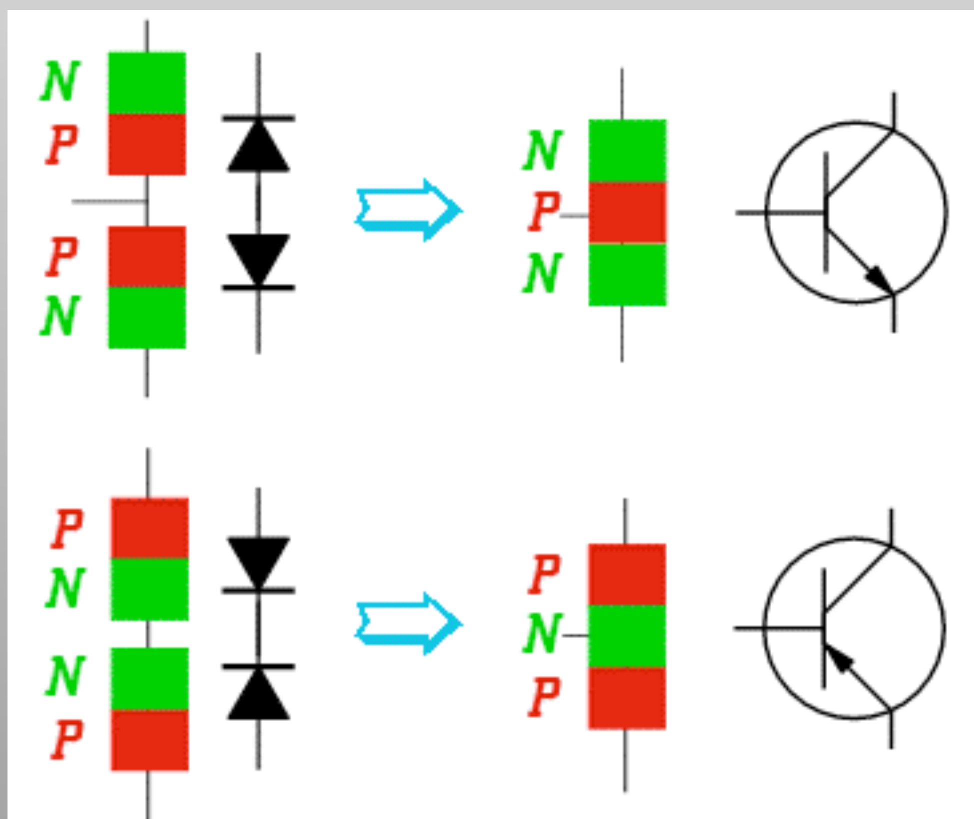


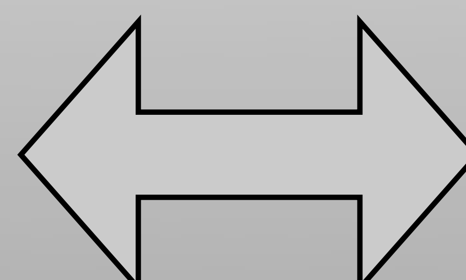


Information and Physics?

- **Information has to be encoded, stored, transmitted, processed and recovered in physical systems;**

- **Physics sets the rules of the game:** Physical laws define what can be done with my source, code, receiver, etc.





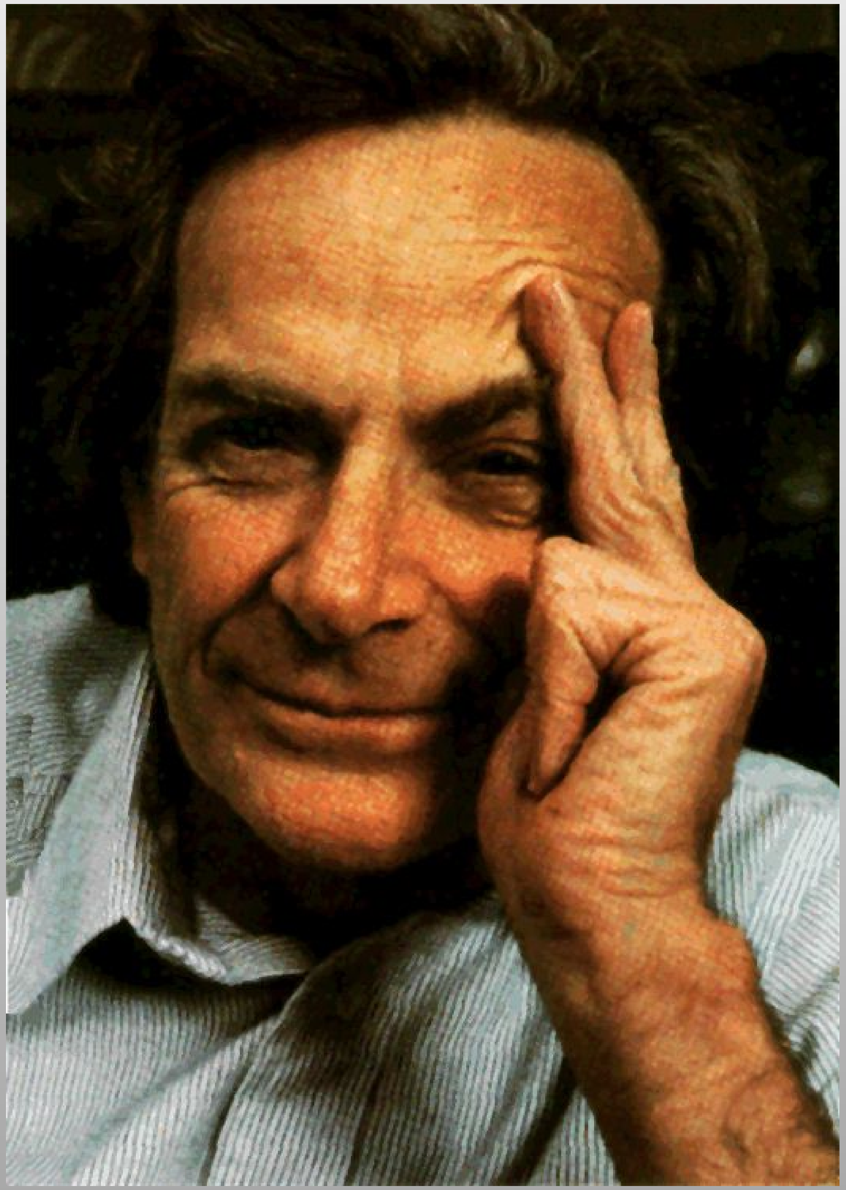
Everything has been done with classical physics... until...

Quantum Mechanics Comes into Play...

"I would like to describe a field... which ... would have an enormous number of technical applications.

What I want to talk about is the **problem of manipulating and controlling things on a small scale**. It is something, in principle, that can be done; but in practice, it has not because we are too big."

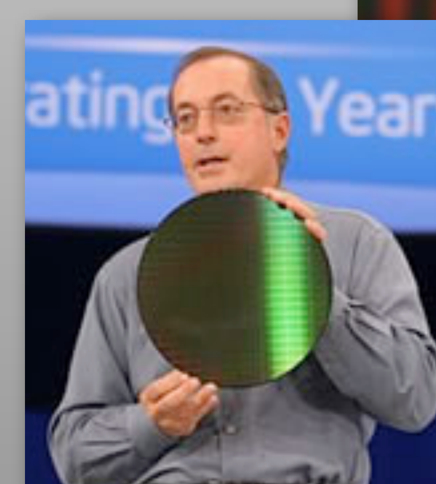
But new experimental capabilities are available!



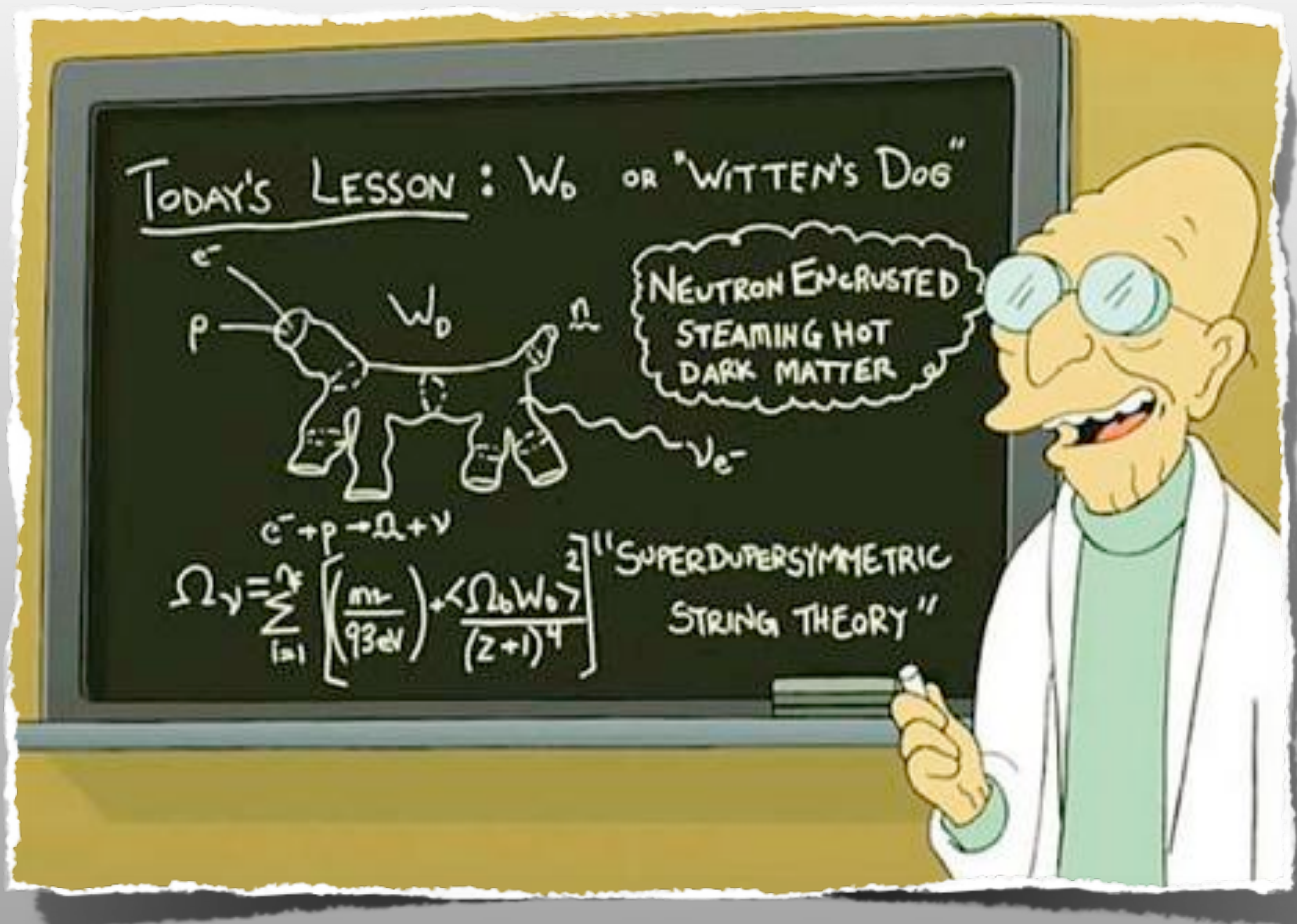
Richard P. Feynman,
There's Plenty of Room at the Bottom
(Caltech, APS Meeting, 29th December **1959**).

Classical Computation has Problems of Size...

- The need for “nano”:
  - Technology is scaling down the size of the components to molecular or atomic dimensions;
  - 45 nm node is commercially available in 2009 in CMOS fabrication. But (e.g.) intel foresees 32 nm, 22 nm, and then 16 nm technology;
  - **Quantum features and effects should start to be considered.**



How do the rules change ???



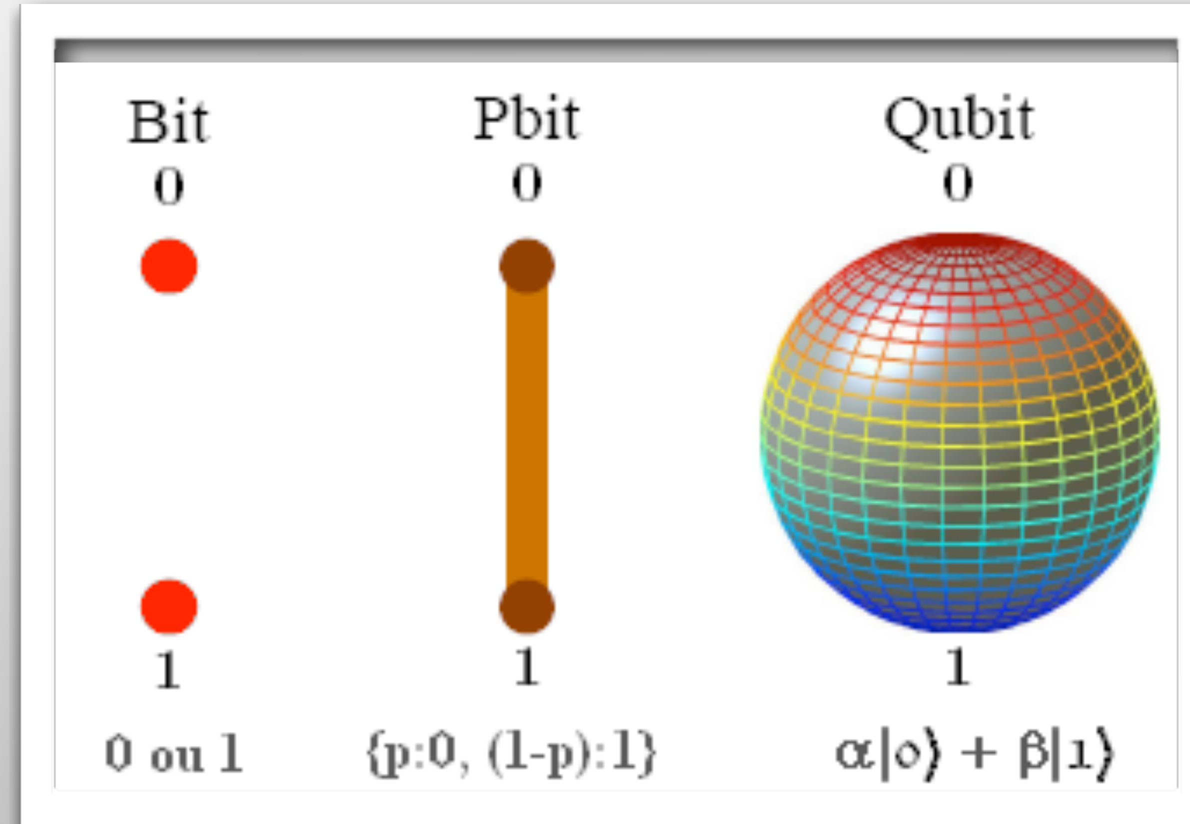
Do I have a chance to understand something?

Classical Bit Vs Quantum Bit

- **Classical Bit:**
  choice over alternatives

  0, 1

  The “state” of the physical system can be either the one corresponding to **1**, or the one corresponding to **0**.



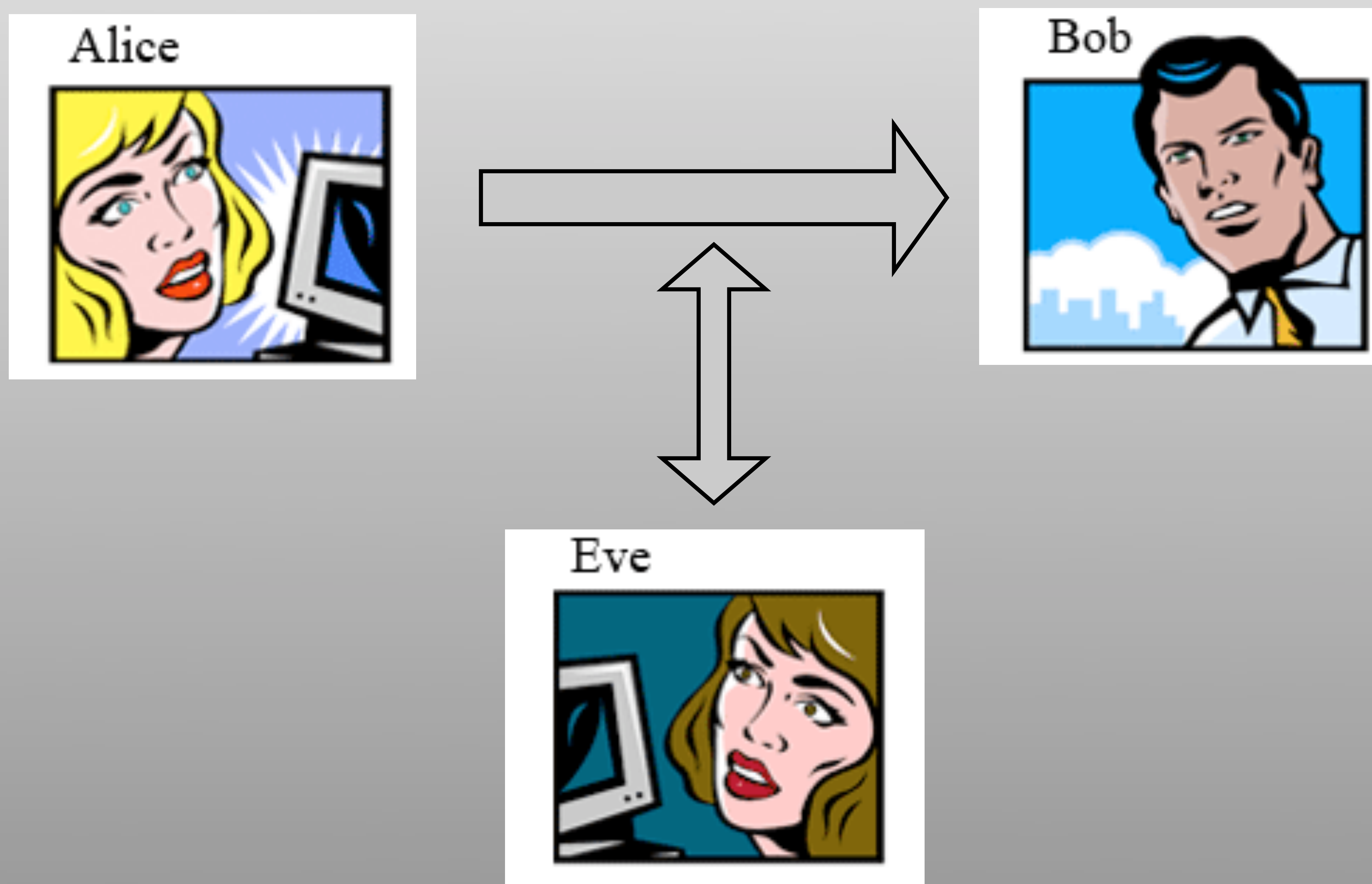
- **Quantum Bit:**
  Quantum Theory allows for Superpositions

  If I have a system with two states **0,1** then all the $\alpha\mathbf{0} + \beta\mathbf{1}$ **are valid, “good” states!**

  Even between different subsystems, even at a distance... it can turn into an advantage!!!

A Key Application: Cryptography

- Basic Setting: A wants to communicate to B without E getting the message...

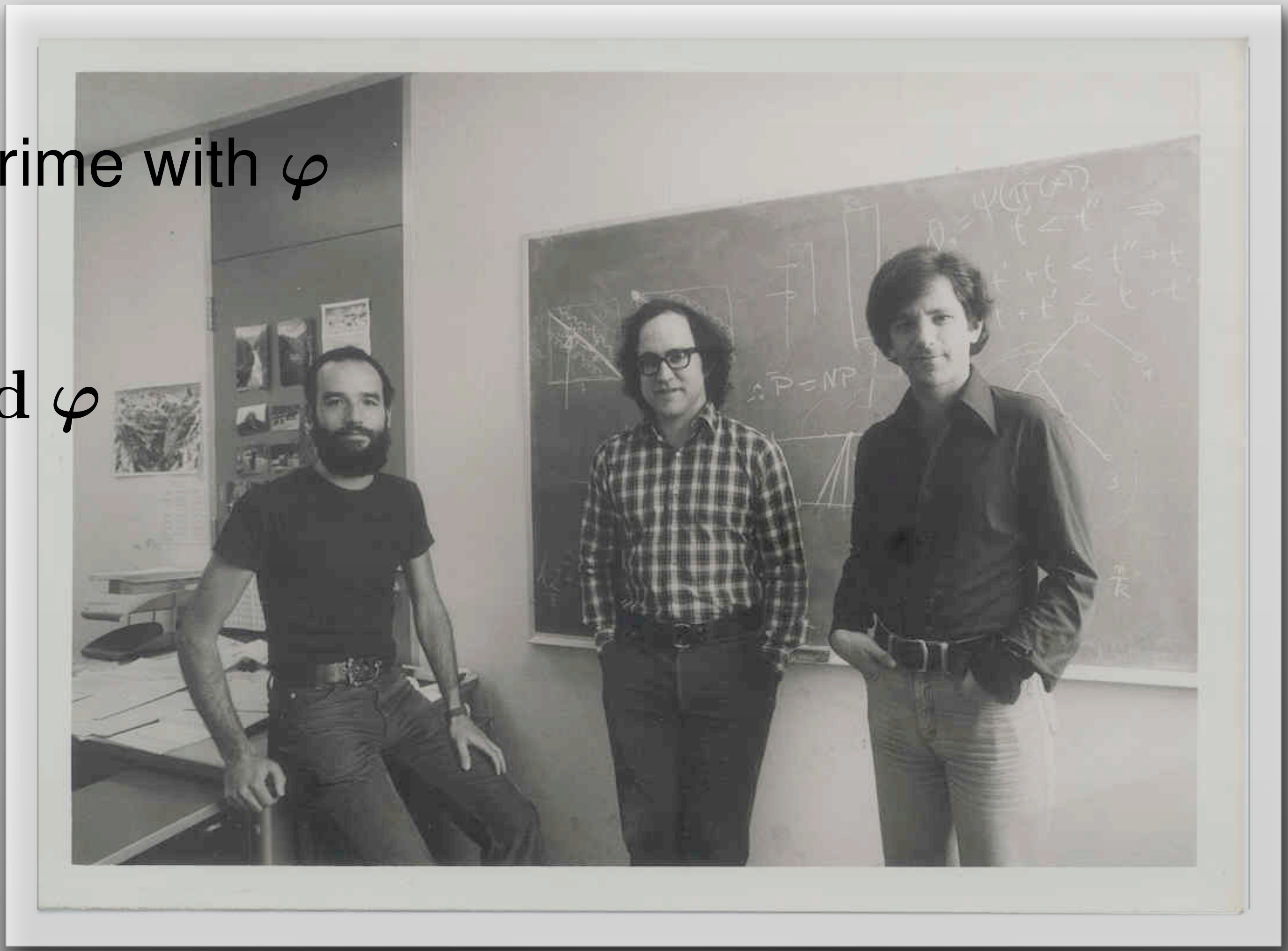


Current methods rely on complexity

Example (cont.)

Public Key: RSA

- Choose two large prime numbers p and q and compute $n = pq$.
- Compute $\varphi = (p-1)(q-1)$
- Choose a positive integer $e < \varphi$ coprime with φ
- (n, e) is the public key.
- Choose an integer d s.t. $de = 1 \bmod \varphi$
- (n, d) is the private key.
- $M < n$: message; C: ciphertext.
- $C = M^e \bmod n$
- $M = C^d \bmod n$

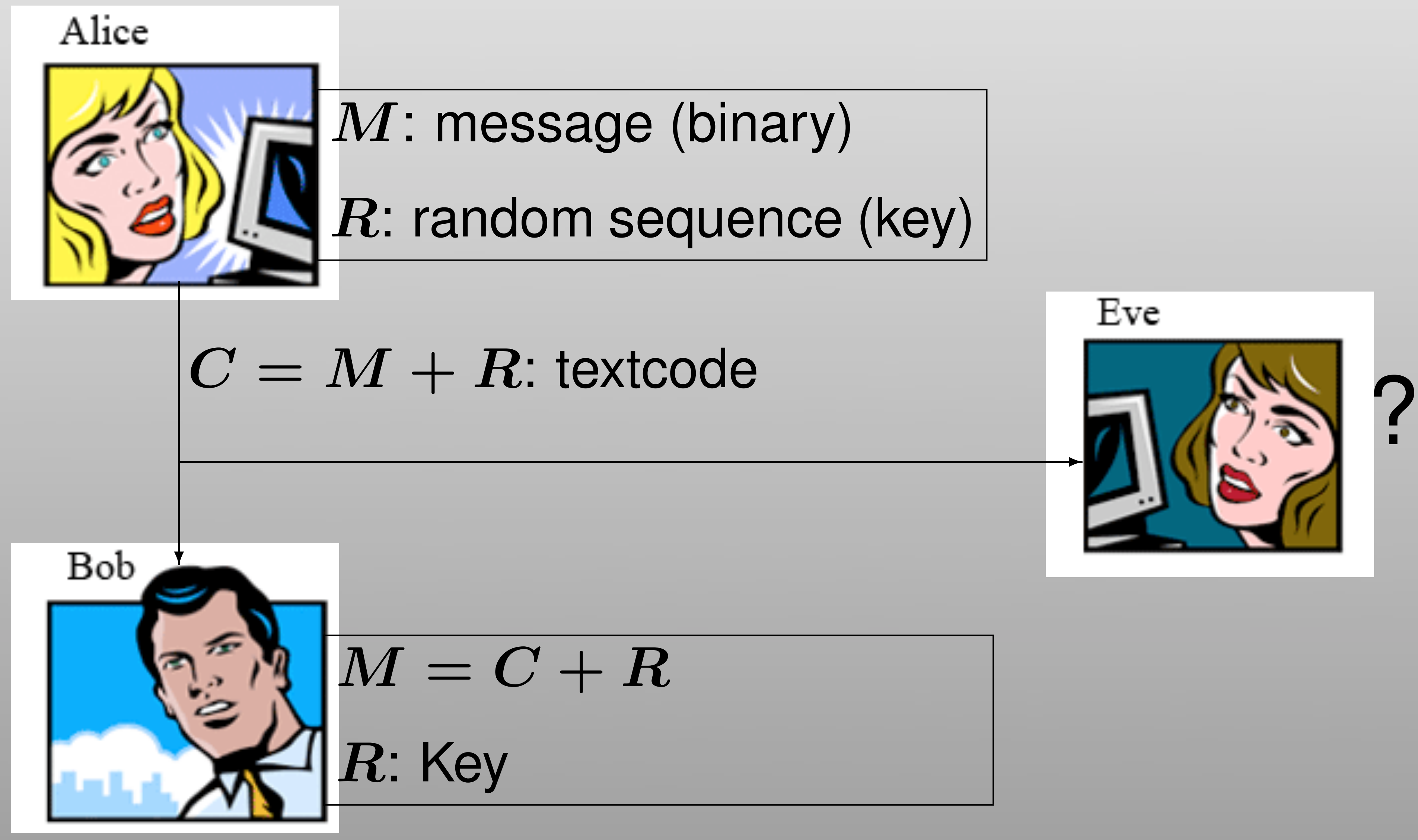


Security based on computational difficulty in factoring n.

Another Approach: Shannon's Idea

Example (cont.)

Unbreakable code (Shannon).



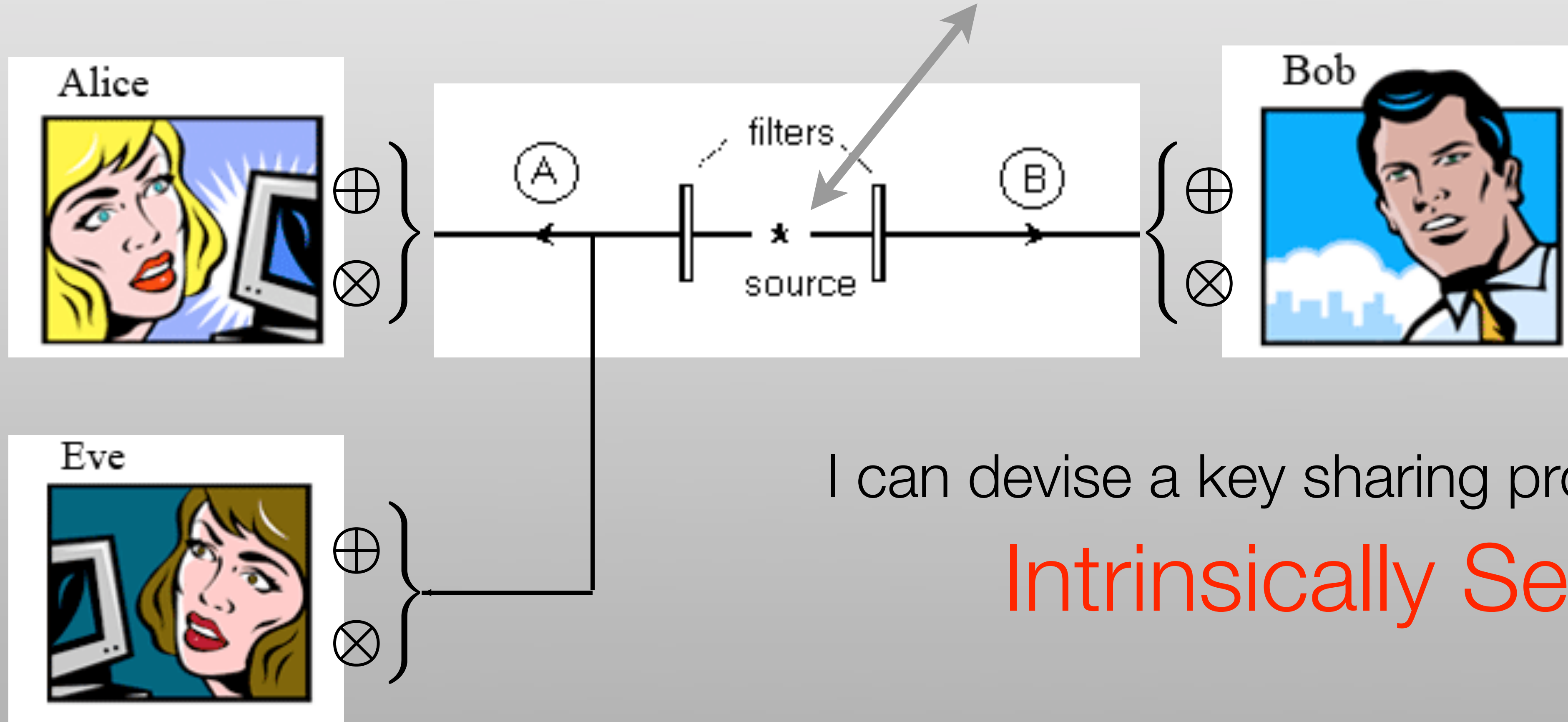
Problem: Key distribution

Quantum Security: Safely Distributing Keys

Example (cont.)

Spotting Eve

source of pairs of photons in non-local superposition states



I can devise a key sharing protocol which is

Intrinsically Secure!

Alice and Bob: ⊕⊕ or ⊗⊗ (different polarization measurements discarded).

If Eve had chosen the same polarization of Alice and Bob (50% of times)$\Rightarrow$ OK

Otherwise: the results of Alice and Bob coincide only 50% of times. $\Rightarrow$

In case of eavesdropping results of Alice and Bob coincide only 75% of times!

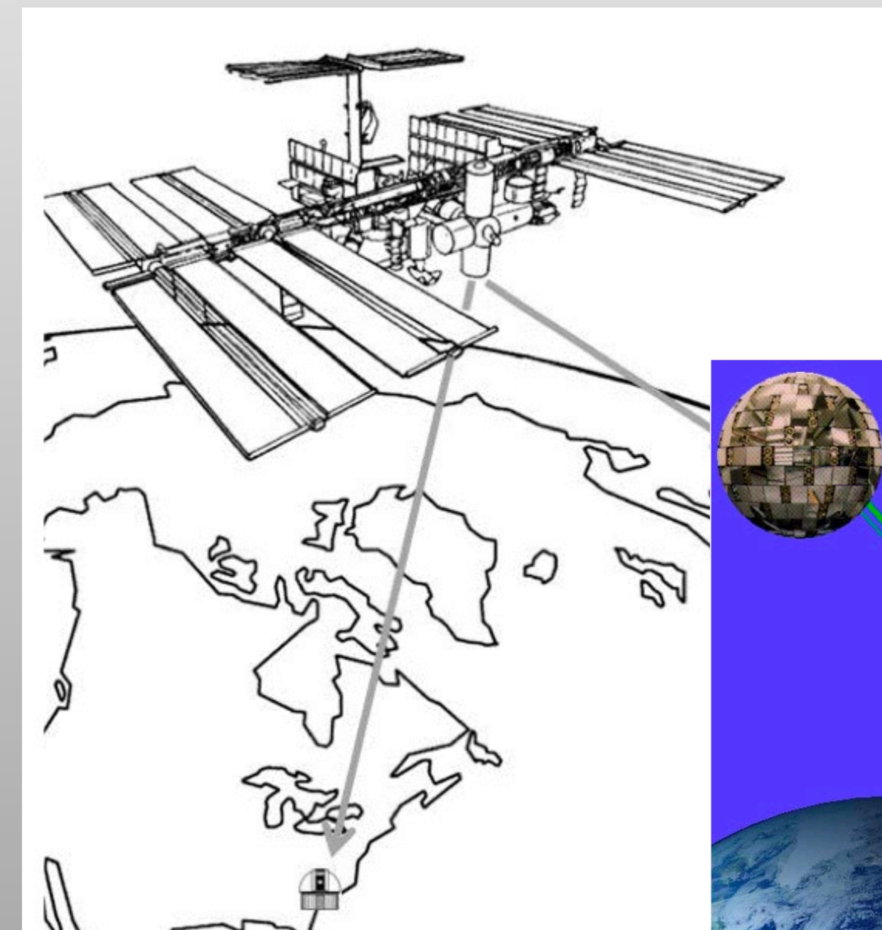
Quantum Future

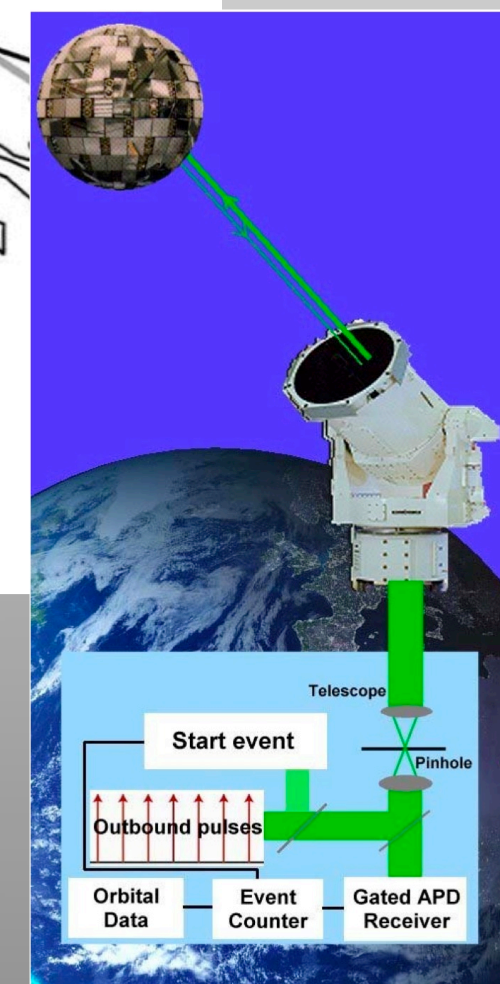
L’Universita` di Padova finanzia la ricerca in comunicazioni quantistiche (Quantum Future ~1.4M Euro)

Al DEI:

caratterizzazione del canale,
teoria di codifica,
compensazione del rumore
progettazione e performance di decodifica,...

... ed esperimenti di comunicazione terra-satellite!





Not only safe quantum key distribution...

Quantum Computers are also promising!!!

They can (could) solve certain difficult problems faster than classical ones:

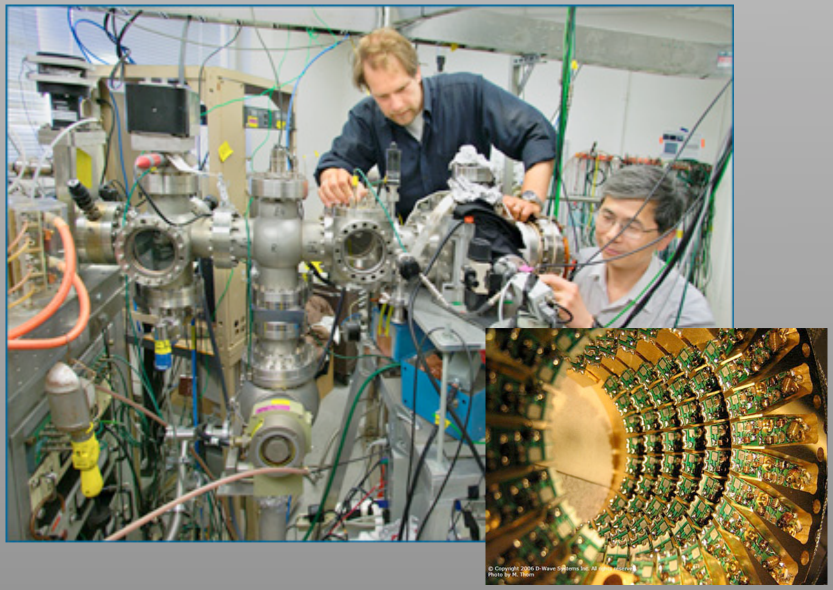
Integer Factorization (Shor);

Unsorted Database Search (Grover);

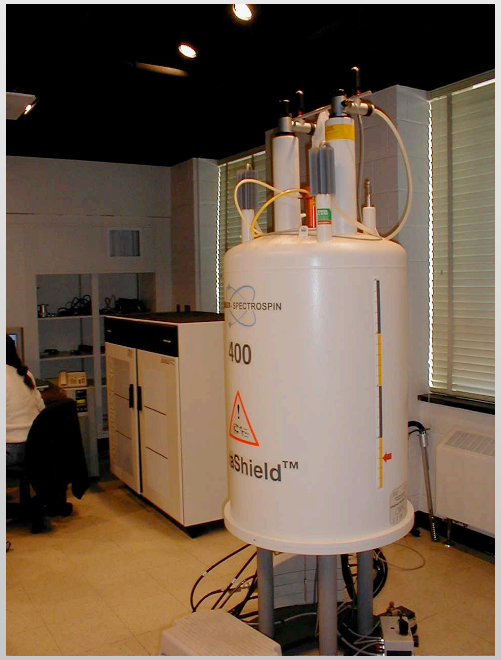
Group Theory problems (...);

Open Problem:

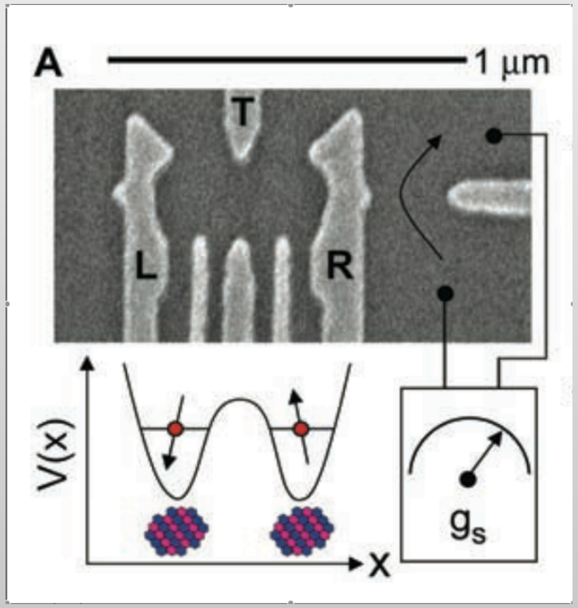
We still don’t know what else !!!



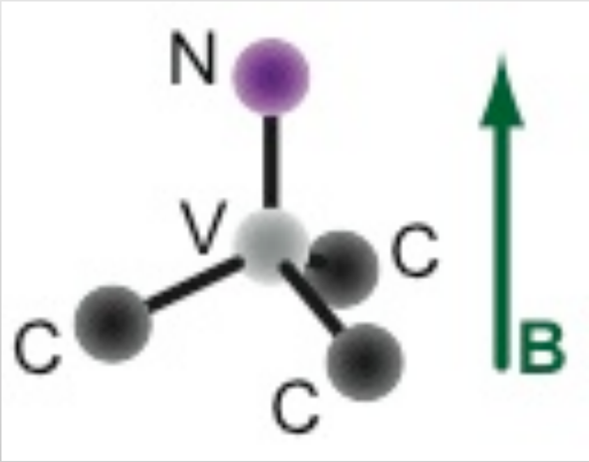
Physical Supports for Quantum Computers



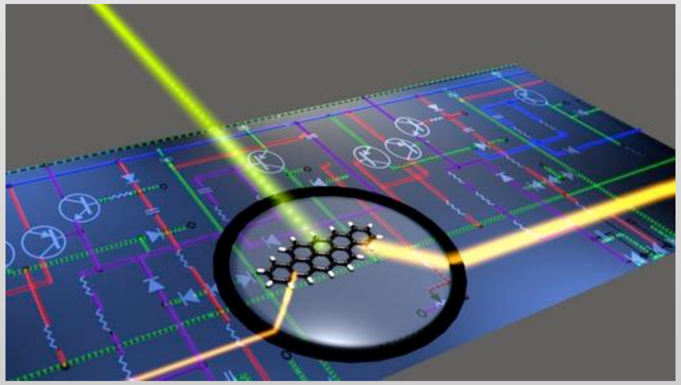
NMR



Quantum Dots



Vacancies in Diamonds
and their spins



Optical Quantum
Circuits

and many others...

Problem 1: Quantum systems are difficult to manipulate...

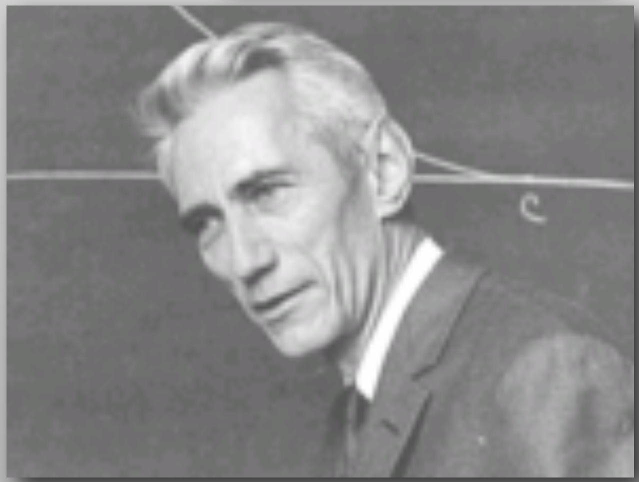
Problem 2: They are small and fragile!

We have to learn how to protect it from the noise...

What do we study...?

i. Controllability, Stability, Feedback, and Robustness for quantum systems
[Quantum Control Theory]

ii. How to encode, store and recover quantum information
[Quantum Error Correction]



iii. How to transmit information and characterize quantum channels
[Quantum Estimation]

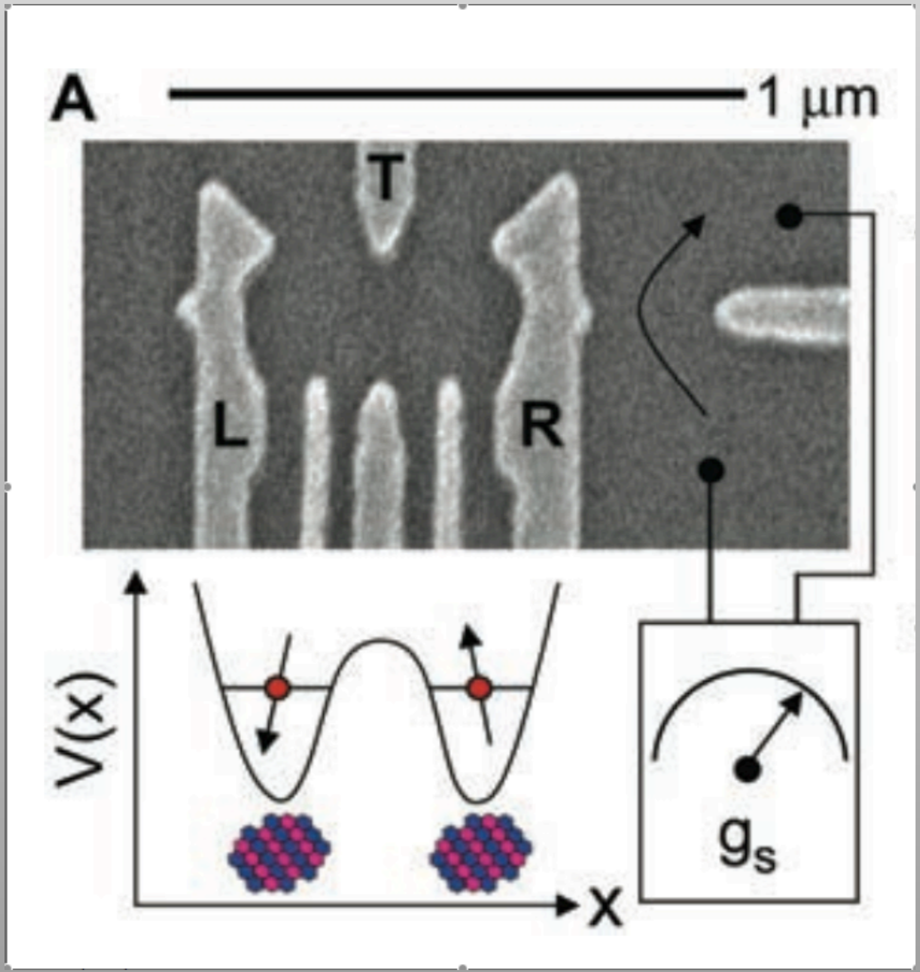
How long can QI survive in a real environment?

- Every real quantum system is immersed in a (quantum) environment:

- Loss of quantum superpositions: Only “classical” information survives.

Example: [Petta & al., Science 05]:

- GaAs quantum dots.
- Confined electrons interact with millions of nuclei through;
- Information lifetime: ~ 10 ns.



- With Decoherence Control: ~1μs

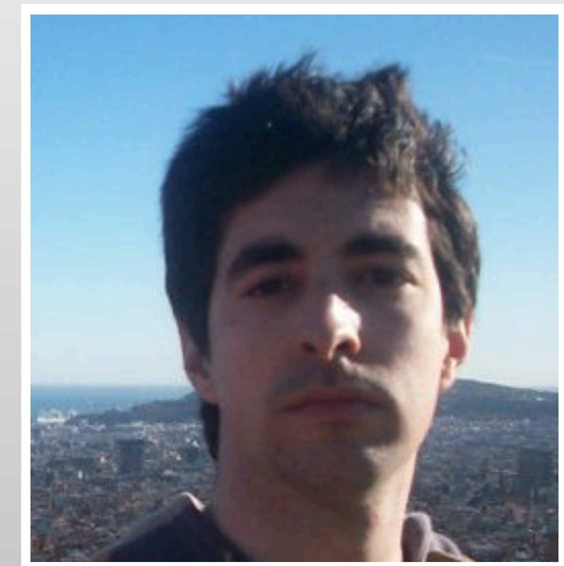
Research Group & Friends

- **System Theory Group**

Francesco Ticozzi

Augusto Ferrante

Michele Pavon



Luca Mazzarella

- **Some collaborations**

P. Villoresi

DEI

C. Altafini

SISSA

L. Viola's group

Dartmouth Coll.

S. Schirmer

Cambridge

P. Cappellaro

MIT

Grazie!

- Disponibile per parlare degli aspetti tecnici...

- ticozzi@dei.unipd.it

- Telefono: 049 827 7603, Ufficio al III piano.