Quantum cryptography, communication, and computing

An elementary introduction

Dimitri Petritis

Institut de recherche mathématique de Rennes
Université de Rennes 1 et CNRS (UMR 6625)

Santiago, November 2013

UNIVERSITÉ DE RENNES 1

Programme of the course I

1. **An extremely brief history of modern Physics.**
   - Why Computer Sciences oblige us to go back to Physics.
   - The emergence of modern physical theories (end of 19th, beginning of 20th century).
   - Status of quantum mechanics.
2. **Postulates of classical mechanics** viewed as classical probability theory with dynamical law.
   - Reducibility of classical randomness.
   - Insufficiency of classical probability to describe nature and the Orsay experiment.
3. **Postulates of quantum mechanics** viewed as an extension of probability theory with a dynamical law. Illustration by a very simple example.

UNIVERSITÉ DE RENNES 1

Programme of the course II

4. **Special topics in Hilbert spaces.**
   - Tensor products of spaces.
   - Classes of operators. Spectral theorem.
   - Partial traces and quantum marginals.
   - Irreducibility of quantum randomness.
   - Complete positivity. Probability projection-valued measures and sharp measurements.
   - Probability positive-operator-valued measures and unsharp measurements.
5. **Principles of quantum cryptography.**
   - In depth presentation of the BB84 protocol.
   - Analysis in case of eavesdropping.
   - Gain of information versus distortion bounds.
6. **Quantum communication protocols:** teleportation, dense coding, ...
7. **Quantum computing:** Period searching and Shor's algorithm for factoring into primes.

UNIVERSITÉ DE RENNES 1

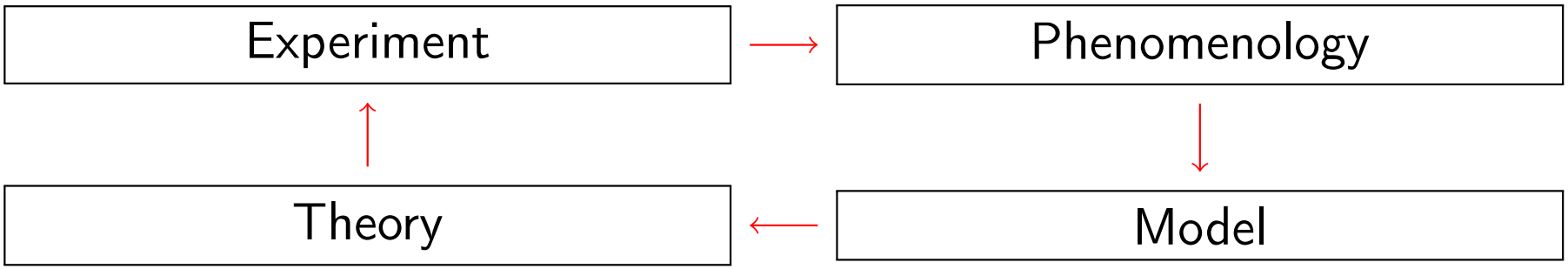
The problem

- Entire domains of scientific (and generally human) activity rely on
  - retrieval,
  - processing,
  - transmission, and
  - **protection**

  of information.
- Nowadays: those steps are algorithmically automated by programmes executed on **reliable electronic devices**.
- We can argue using the **abstract mathematical categories** of **logical circuits** of a computer without paying attention to the physical layer on which these programmes are executed.
- Because we can still do so! But we must already now start caring about the physical layer.

UNIVERSITÉ DE RENNES 1

Physics is an experimental science



Blackboard 1: Classical mechanics, electromagnetism, statistical mechanics

- Physical theories have **finite life span**; accepted as long as not contradicted by experiment.
- Physical truth based on **experiment**.
  - careful preparation of the system into a **state**,
  - interaction of the system with carefully designed **measuring apparatus**,
  - recording **results**.
- Consequences of experimental nature of Physics
  - statistical **errors** but statistical **reproducibility**,
  - **perturbation** induced by measuring apparatus can be made **negligible**,
  - Physics must be **universal**.
- In the quest of universality, Physics has an ally: Mathematics.

UNIVERSITÉ DE RENNES 1

- Physics uses Mathematics to formulate concepts and make quantitative predictions.
- Mathematics develops new tools inspired from physical problems.
- Mathematical Physics is
  - Physics: statements to be verified by experiment, and
  - Mathematics: statements to be derived as theorems based on small number of axioms (postulates).

Blackboard 2: Examples.

Stories of false certainties and sheer arrogance

- By end of 19th century: "Physics is finished as a fundamental science"; only some minor problems to solve.
- Young people advised not to loose their time with Physics but look towards . . . finance or technology.
- But, hold on a minute!
CM	local	$\mathbf{x}' = g \cdot \mathbf{x};\ t' = t$	$g \in O(3)$
	full	$\mathbf{x}' = \mathbf{x} + \mathbf{a};\ t' = t + s$	Galileo group
EM	local	$(t', \mathbf{x}') = g \cdot (t, \mathbf{x})$	$g \in O(1,3)$
	full	$(t', \mathbf{x}') = (t, \mathbf{x}) + (s, \mathbf{a})$	Poincaré group
- Why 2 different groups of invariance?

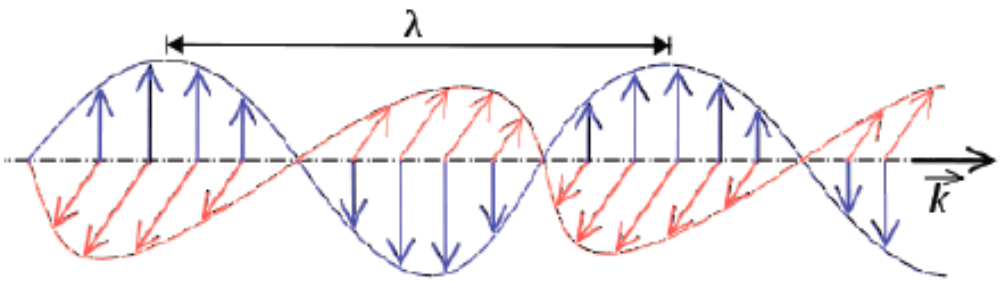
UNIVERSITÉ DE RENNES 1

- A . . . little problem: Maxwell equations.

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\epsilon_0} \quad ; \quad \nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$
$$\nabla \cdot \mathbf{B} = 0 \quad ; \quad \nabla \times \mathbf{B} = \mu_0(\mathbf{J} + \epsilon_0 \frac{\partial \mathbf{E}}{\partial t})$$

- In vacuum: $\rho = 0$; $\mathbf{J} = 0$; $c^{-2} = \epsilon_0 \mu_0$.

$$\mathbf{E} = \mathrm{Re}(\mathbf{a} \exp(2\pi i(z - ct)/\lambda)); \mathbf{B} = \mathbf{a} \times \mathbf{E}; \mathbf{a} = \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{pmatrix}.$$



(Figure from A. Childs, Introduction to quantum mechanics)

End of 19th, beginning of 20th century

Everything is falling down II

- Michelson-Moreley experiments (1887, 1902–1905): Aether does not exist!
- Becquerel (1896) discovers radioactivity: matter is not stable!
- Boltzmann, Thomson, Einstein, Perrin (1897–1908) establish existence of atoms: matter is not continuous!

UNIVERSITÉ DE RENNES 1

End of 19th, beginning of 20th century

Everything is falling down III

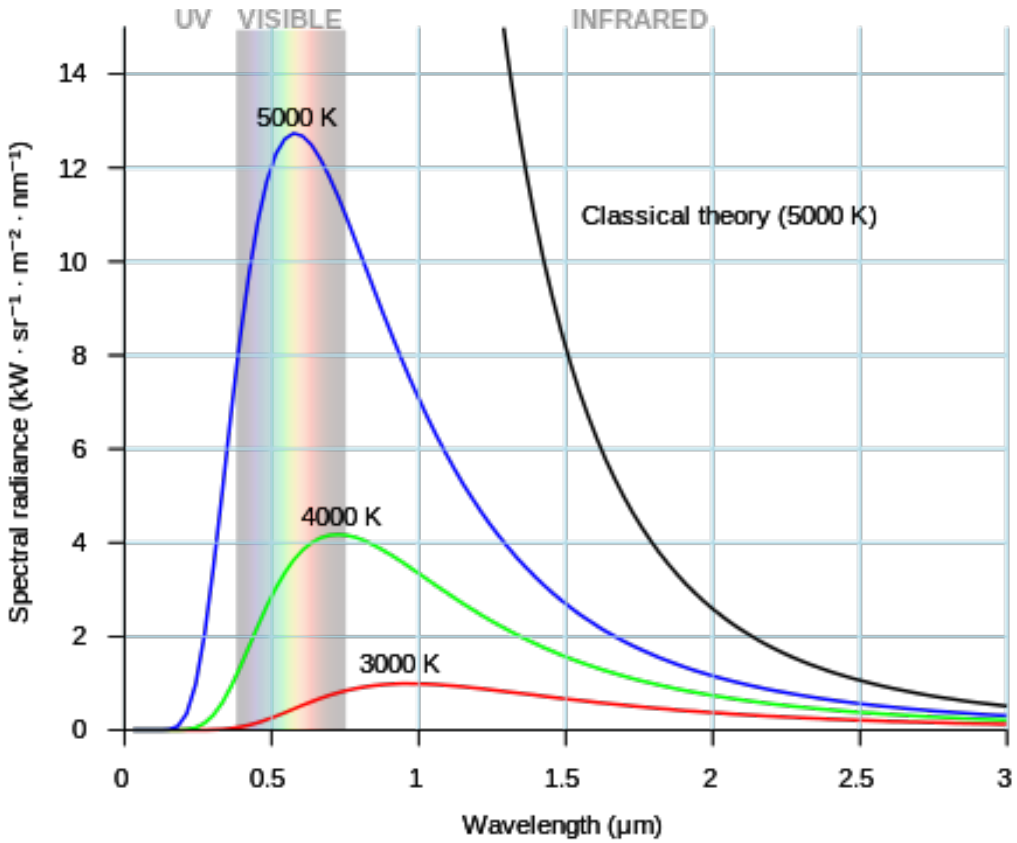


Figure: Classical theory (Rayleigh) of black-body radiation not in accordance with experiment (source of figure: wikipedia).

- Planck (1900) gives groundbreaking phenomenological explanation of black-body radiation: energy levels must be discrete.
- Einstein (1905) establishes special relativity: unifying classical mechanics and electormagnetism. Based on two simple principles.
  - Speed of light c is a universal constant, the same in all reference frames.
  - Laws of physics identical in all inertial frames.

  Consequences: no need of aether but space and time are not absolute!
- Bohr, Heisenberg, Pauli, Dirac, Schrödinger, von Neumann (1913–1932) consider Planck's idea seriously and establish Quantum Mechanics: energy is not continuous but "quantified".

UNIVERSITÉ DE RENNES 1

A general physical theory
must describe any phenomenon in the Universe

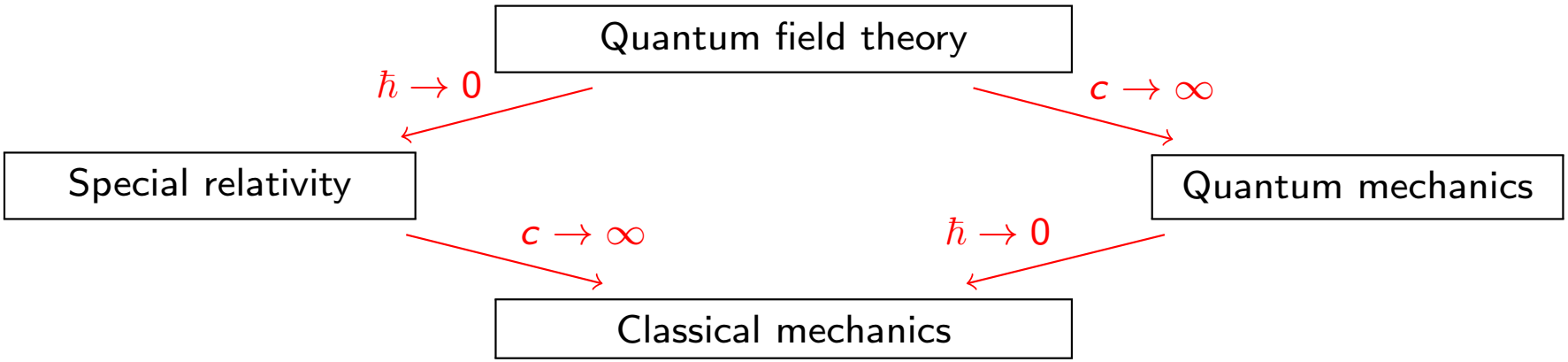
- Measure units introduced during French Revolution for everyday quantities to have reasonable numerical values, typically $10^{-3} - 10^{3}$.
- Length l: 10^{-15}m (proton radius) – 10^{26}m (radius of the universe).
- Mass m: 10^{-30}kg (electron mass) – 10^{50}kg (mass of the universe).
- Time t: 10^{-23}s (time for light to cross atomic nucleus) – 10^{17}s (age of the universe).

UNIVERSITÉ DE RENNES 1

Quantum field theory

Two physical constants:

- Planck's constant $\hbar = 10^{-34}$Js,
- speed of light in vacuum $c = 3 \times 10^8$m/s.



Can we ignore Quantum Mechanics?

NO!

UNIVERSITÉ DE RENNES 1

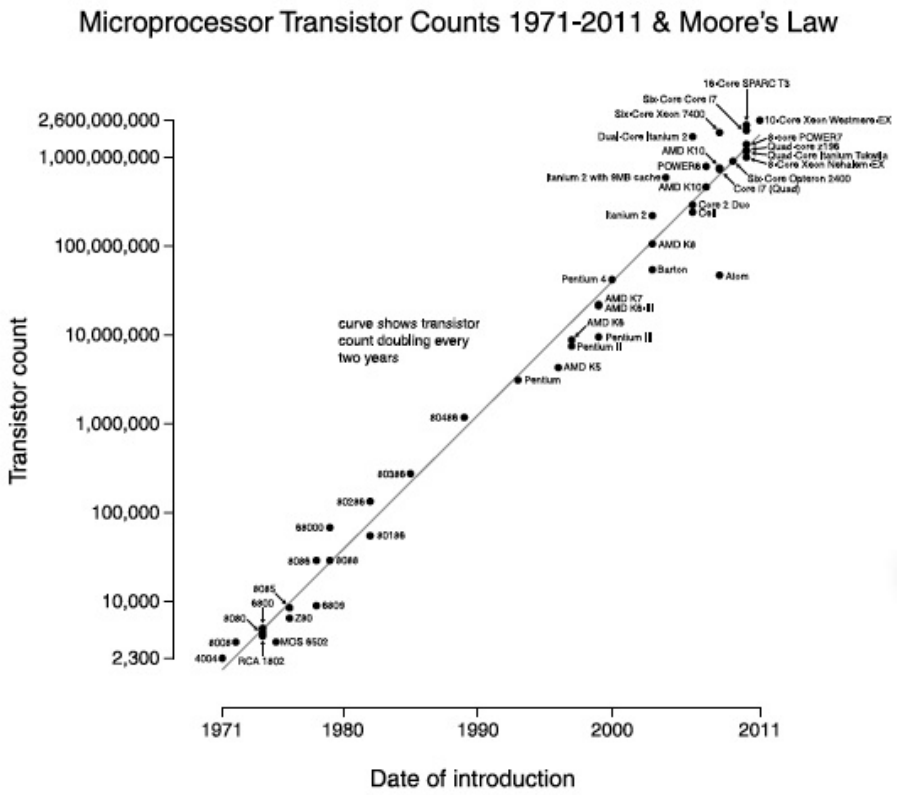
Yes, we can!

1/3 of world economy relies on technological applications stemming from quantum phenomena. E.g.

- Laser: CD, DVD, fiber optics communications, surgery, metallurgy, ...
- Superconductivity: high magnetic fields, Meissner effect and magnetic levitation, ...
- Quantum tunnelling: field effect microscope and applications into nanotechnology (cancer cell invasion driven by specificity), fullerenes, ...
- Quantum cryptography and communication: inviolable quantum cryptologic protocols, superdense coding, teleportation of quantum states, ...

UNIVERSITÉ DE RENNES 1

What we learn from history?
Projection to the future (transistors count)



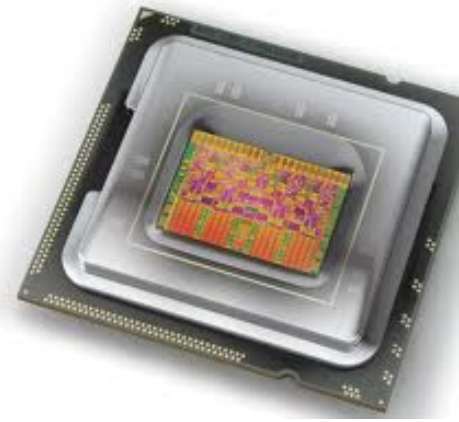
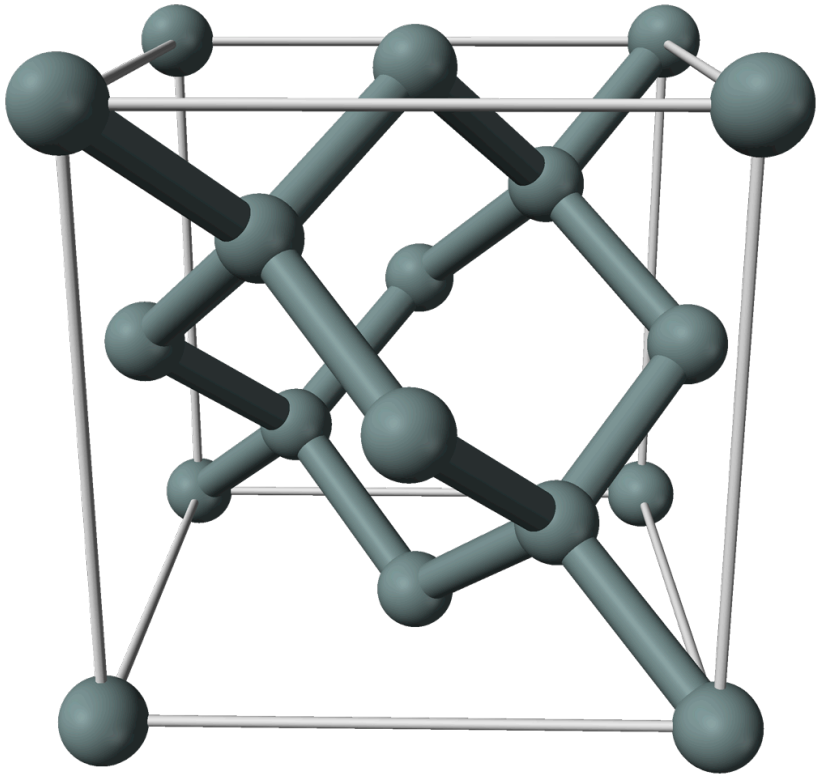


Figure: **Gordon Earl Moore** (San Francisco, CA, 1929 –), the marine's officer who proposed the so called "Moore's law" (in the middle) and one of most recent microprocessors (Intel Core I7 Nehalem (2008), with a surface of 263 mm^2). (Source of figures and data: Wikipedia)

Silicium (Si) = solid crystallising in the "diamond" shape.
Periodic repetition of a cube having edges of $a = 0.5431$ nm.
Interatomic distance $\frac{\sqrt{3}}{4}a = 0.2352$ nm.



UNIVERSITÉ DE RENNES 1

What we learn from history?
Projection to the future (etching thickness)

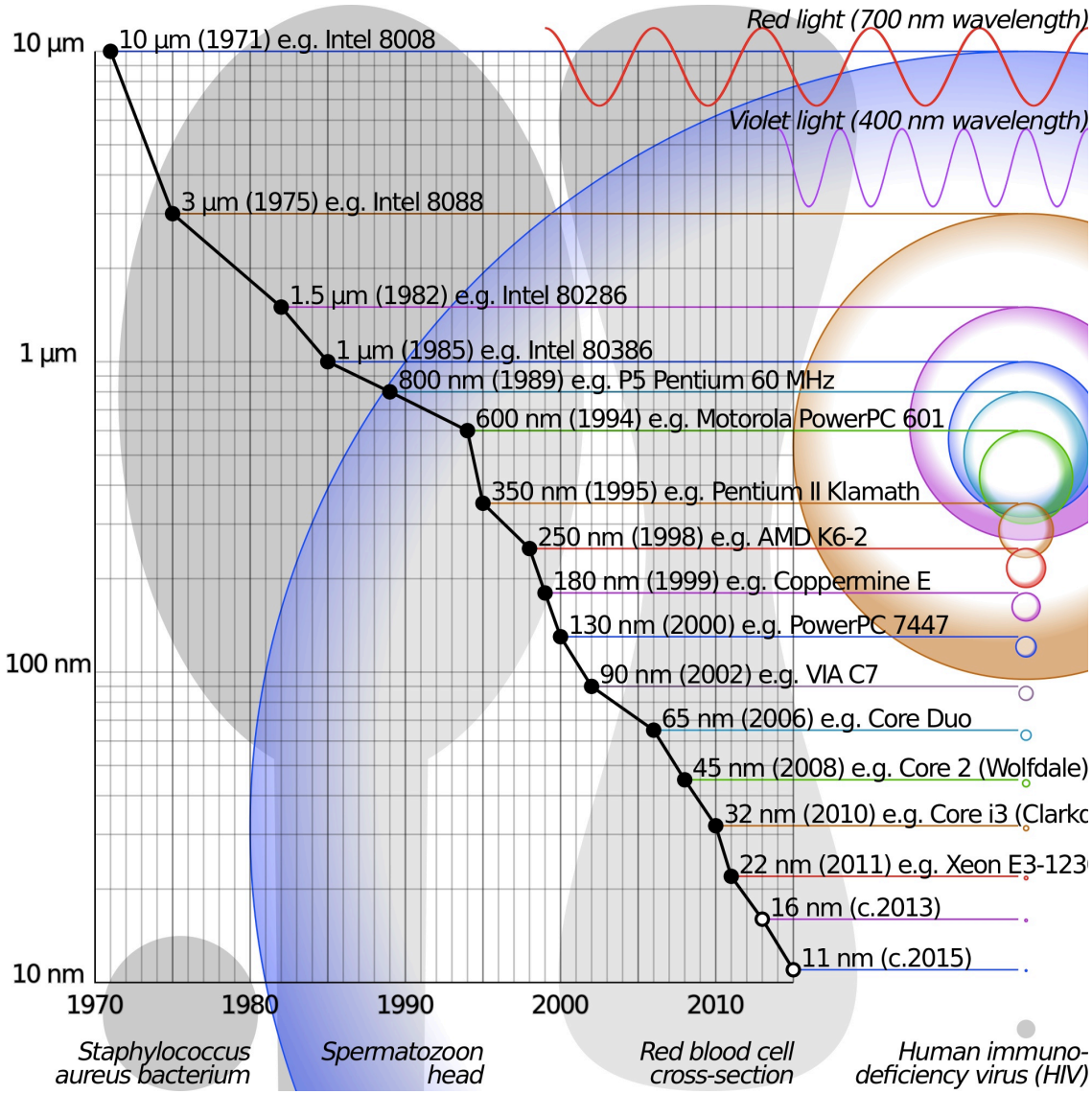
Date	Nom	Nombre de transistors	Finesse de gravure (nm)	Fréquence de l'horloge	Largeur des données	MIPS
1971	Intel 4004	2 300	10000	108 kHz	4 bits/4 bits bus	0,06
1974	Intel 8008	6 000	6000	2 MHz	8 bits/8 bits bus	0,64
1979	Intel 8088	29 000	3000	5 MHz	16 bits/8 bits bus	0,33
1982	Intel 80286	134 000	1500	6 à 16 MHz (20 MHz chez AMD)	16 bits/16 bits bus	1
1985	Intel 80386	275 000	1500	16 à 40 MHz	32 bits/32 bits bus	5
1989	Intel 80486	1 200 000	1000	16 à 100 MHz	32 bits/32 bits bus	20
1993	Pentium (Intel P5)	3 100 000	800 à 250	60 à 233 MHz	32 bits/64 bits bus	100
1997	Pentium II	7 500 000	350 à 250	233 à 450 MHz	32 bits/64 bits bus	300
1999	Pentium III	9 500 000	250 à 130	450 à 1 400 MHz	32 bits/64 bits bus	510
2000	Pentium 4	42 000 000	180 à 65	1,3 à 3,8 GHz	32 bits/64 bits bus	1700
2004	Pentium 4 D (Prescott)	125 000 000	90 à 65	2.66 à 3,6 GHz	32 bits/64 bits bus	9000
2006	Core 2 Duo (Conroe)	291 000 000	65	2,4 GHz (E6600)	64 bits/64 bits bus	22000
2007	Core 2 Quad (Kentsfield)	2*291 000 000	65	3 GHz (Q6850)	64 bits/64 bits bus	2*22 000 (?)
2008	Core 2 Duo (Wolfdale)	410 000 000	45	3,33 GHz (E8600)	64 bits/64 bits bus	~24 200
2008	Core 2 Quad (Yorkfield)	2*410 000 000	45	3,2 GHz (QX9770)	64 bits/64 bits bus	~2*24 200
2008	Intel Core i7 (Bloomfield)	731 000 000	45	3,33 GHz (Core i7 975X)	64 bits/64 bits bus	?
2009	Intel Core i5/i7 (Lynnfield)	774 000 000	45	3 06 GHz (I7 880)	64 bits/64 bits bus	76383
2010	Intel Core i7 (Gulftown)	1 170 000 000	32	3,47 GHz (Core i7 990X)	64 bits/64 bits bus	147600
2011	(Sandy Bridge)		32			
2012	Intel Core i3/i5/i7 (Ivy Bridge)		22			

For comparison:

- thickness of human hair 100μm,
- 0.032μm= 32nm (2010),
- 0.016μm= 16nm (2013 - source Intel),
- 0.011μm= 11nm (expected in 2015 - source Intel).
- interatomic distance of silicium 235.2pm$\simeq$ 0.2352nm.

UNIVERSITÉ DE RENNES 1

What we learn from history?
Projection to the future (etching thickness)



p et q large primes, $N = pq$, $n = \log N$

- Beginnings of RSA protocol (1978), $\tau = \mathcal{O}(\exp(n))$.
- Lenstra-Lenstra (1997), $\tau = \mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$.
- Shor (1994), if a quantum computer existed $\tau = \mathcal{O}(n^3)$.

Very rough estimation: 1 operation par nanosecond, $n = 1000$

$\mathcal{O}(\exp(n))$	$\mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$	$\mathcal{O}(n^3)$
10^{417} yr [1]	0.2 yr	1 s

[1] For comparison: age of the universe 1.5×10^{10} yr