# Quantum Technologies : objectives, prospects and challenges

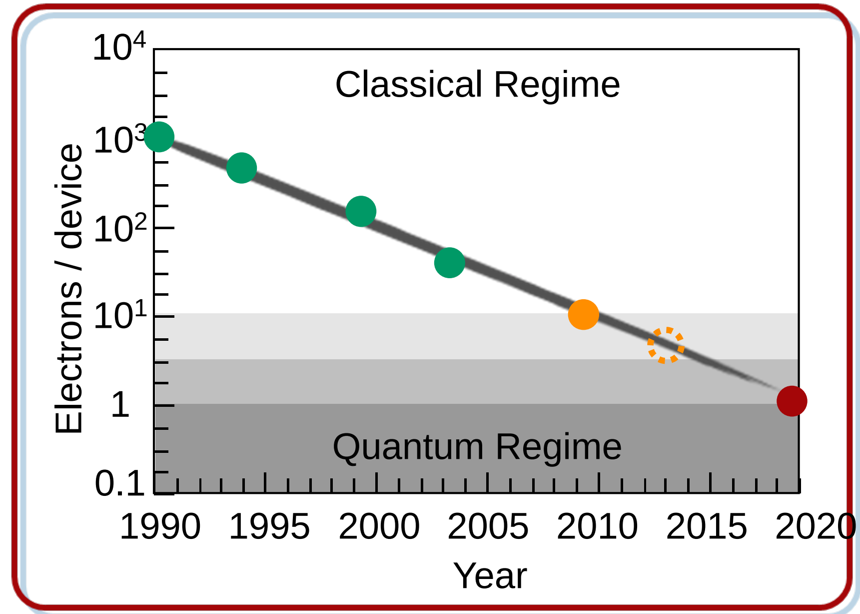
Elisabeth Giacobino
Ecole Normale Supérieure,
Université Pierre et Marie Curie,
Centre National de la Recherche Scientifique,
Paris, France

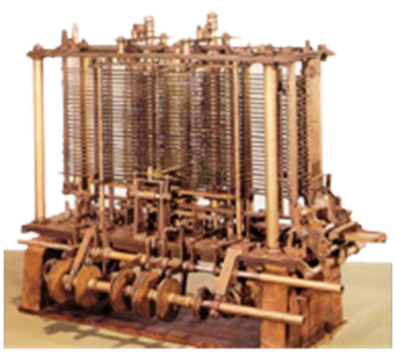
Member of ISTAG
(Information Society Technology Advisory Group)

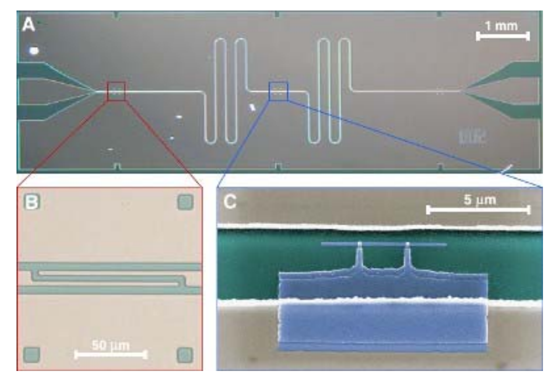
Rainer Blatt
Vladimir Buzek
Tommaso Calarco
Elisabeth Giacobino
Philippe Grangier
Peter Zoller

# the future
# IS quantum

- Moore's law: the number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years
  - Driving force of technological and social change in the late 20th and early 21st centuries
- Eventually the quantum wall will be hit
  - Not a question of if rather of when
  - Push back the hitting time (more Moore) and/or change completely the technology (more than Moore)



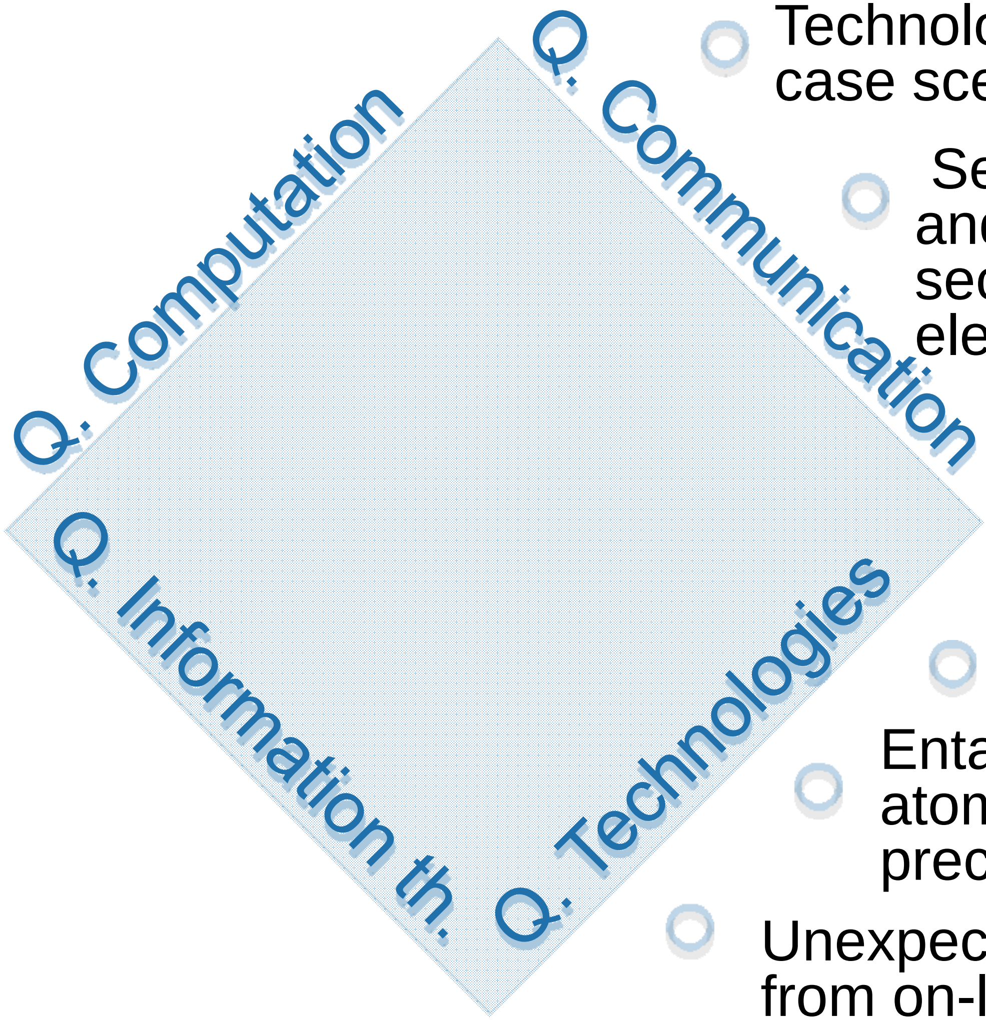






"quantum information is a radical departure in information technology, more fundamentally different from current technology than the digital computer is from the abacus".

W. D. Phillips, 1997 Nobel laureate
member of the AQUTE Integrating Project

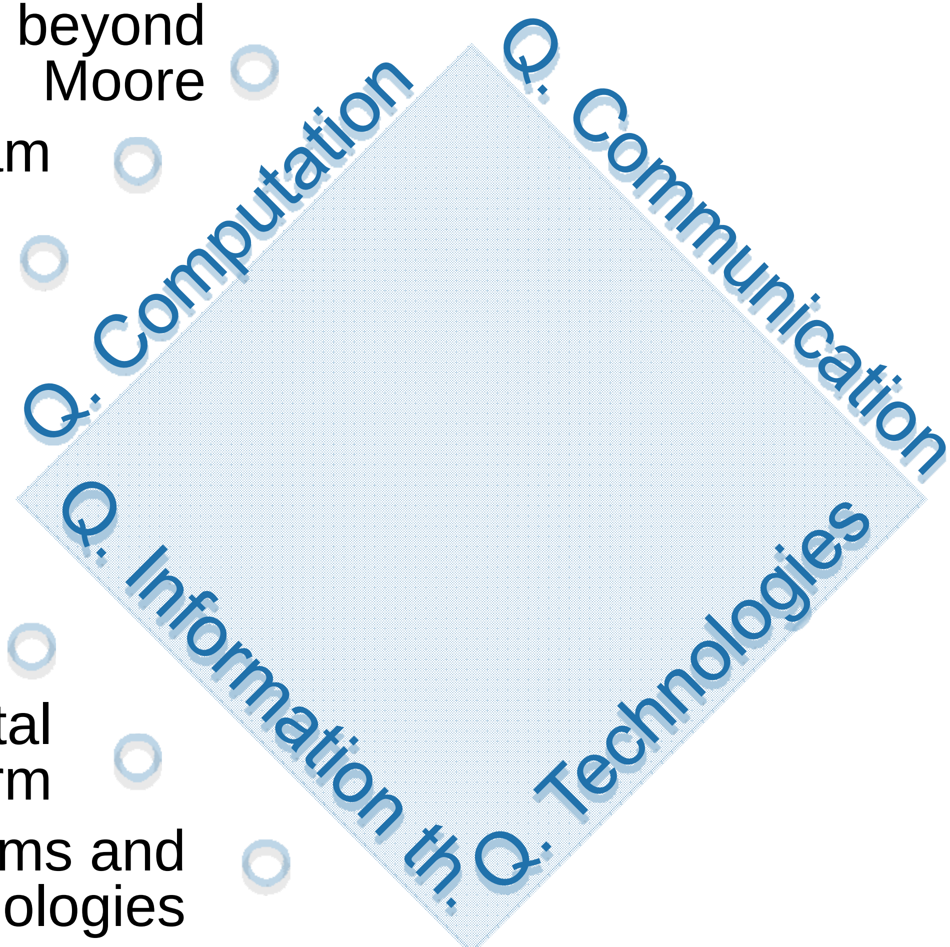
# QIPC areas




- Technology ready to be deployed in real case scenarios
- Several SMEs use quantum techniques and quantum cryptography. It was used to secure the results of a Swiss federal elections in 2007
- Standardization process started
- Technologies enabled by harnessing entanglement
- Entanglement allows for much better atomic clocks and therefore more precision in GPS
- Unexpected markets : QRNG customers are from on-line gambling and lotteries

# QIPC areas

- One of the most promising route beyond Moore
- Still upstream
- but few qubits special purpose processors (quantum simulators) are on sight
- Major driver for the development of the field (e.g., BB84, Shor)
- Guide and support for experimental platform
- Inspiration for new protocols pardigms and technologies



timeline for
# quantum computation

t=0

t=10

t=20

- 1981. First idea: Feynman quantum simulator

  -14 y

- 1995. Shor’s algorithm; Cirac-Zoller gate
  Start of quantum computation

  5 y

- 2000. Diverse approaches
  (Trapped ions, neutral atoms, cavity QED, semiconductor, superconducting, linear optics, impurity spins, single molecular cluster, NMR,...)

  7 y

- 2002. 2-qubit gates

  11 y

- 2006. Quantum byte (trapped ions)

  13 y

- 2008. Error correction threshold reached

  18 y

- 2013. Few qubit quantum processors
  Quantum simulators

  >25 y

- >2020. General purpose quantum processors

Too early to pick up the winning implementation technology
(still true, see e.g., hybrid techs)

timeline for
# quantum communications

t=0
t=10
t=20

## QKD
point-to-point < 400Km

- 1984. First idea BB84
- 1991. Ekert PRL; start of quantum information
- 1992. First experiment
- 1993. Diverse approaches
- 1995. Out of lab
- 2001. id Quantique start-up
- 2008. Autonomous operations
- 2012. Mbps @ 50Km

## Q REPEATERS
network and > 400Km

- 1998. First idea: Briegel et al
- 2005. Diverse approaches (REI, NV, Atoms, Gases)
- 2007. First experiment (Atom gas and ions)
  Multi-mode memory idea
- 2013. First functional quantum repeater link
- 2020. Out of lab

QIPC
# scientific challenges

Source:
Quantum Information Processing and Communication: Strategic Report on current status, vision and goals for research in Europe
Version 1.7, April 2010

## Quantum Computation

short term (~5y)

- Devices realizing quantum algorithms with up to 10 qubits
- Fault tolerant computing and error correction on small scale systems
- Distributed quantum algorithm
- Different classes of entangled states up to 10 qubits
- Quantum simulation of a system that cannot be simulated classically

long term (~10y)

- Large dimension quantum memory
- Quantum algorithm with up to 50 qubits
- Quantum simulation of a key problem in science
- Quantum algorithm with fault tolerant error correction

## Quantum Commmunication

short term (~5y)

- Build a quantum repeater with two nodes
- Interface photons with matter
- Secure quantum key distribution network

long term (~10y)

- Satellite quantum communication
- 1000 km quantum cryptography
- Multi-node quantum networks
- Realization of new quantum protocols

# QIPC scientific challenges

Source:
Quantum Information Processing and Communication: Strategic Report on current status, vision and goals for research in Europe
Version 1.7, April 2010

short term (~5y)

long term (~10y)

## Quantum Technologies

- Develop entanglement based technologies, e.g.,
  - Clocks
  - Metrology
- Develop entanglement enhanced technologies, e.g.,
  - Sensors
  - Imaging, photonics
- Entanglement enabling quantum control
- Entanglement system engineering

---

- Quantum simulator as a scientific tool
- Bootstrap the quantum technologies market

## Quantum Information Theory

- Develop
  - Computation paradigms and algorithms
  - Communication protocols
  - Quantum specific techniques (e.g., quantum control and feedback methods)
- Guide and support experimental developments, covering the widest possible range of physical systems and technologies.

Roadmap Quantum information processing and communication
http://qurope.eu

# quantum computation

- New components and devices that will be elements in the long term in high-performance computing facilities

  It will provide

  - Quantum processors
  - Quantum simulators
  - Hybrid technologies

# quantum communication

- New components and devices that will be elements in the long term in high-performance computing facilities

  It will provide

  - Global scale quantum communication (security, privacy)
  - Quantum internet
  - Wiring of quantum processors

# quantum technologies

- New technologies ready for a market where the quantum limits will define the performance of industrial applications

  It will provide

  - Global scale quantum communication (security, privacy)
  - Disruptive photonics devices (e.g.,single photon detectors, quantum repeaters)
  - Metrology, sensors, imaging
  - Quantum simulators

# quantum information theory

- Guide and support experimental developments, covering all range of physical systems and technologies

  Il will provide

  - Computational paradigms, algorithms and optimized techniques
  - Communication protocols
  - Inspiration for new technologies

# Conclusion

“**Quantum Information Technologies hold the promise of revolutionizing computing and communication**.
FET invested early in these mind boggling technologies and rallied a group of Member States to match its efforts.
Thank to this support, Europe now produces half of the scientific knowledge worldwide in this area and leads the commercial exploitation of this technology in the area of network security.
What was considered fiction less than a decade ago, has become a reality today.”

V. Reading, Commissioner DG-INFSO
opening address of the FET “Science Beyond Fiction” conference (Prague, 2009)