Imperial College London

IBP event Quantum Technologies – 29 November 2017

The Road to Quantum Computers

Mario Berta (Department of Computing and QuEST Imperial)

marioberta.info – mathematical aspects of quantum information science

Imperial College London

Quantum Information Science

- Understanding quantum systems (e.g., single atoms or electrons) is hard

Richard Feynman
(The Nobel Foundation)

Understanding physics with computers '81

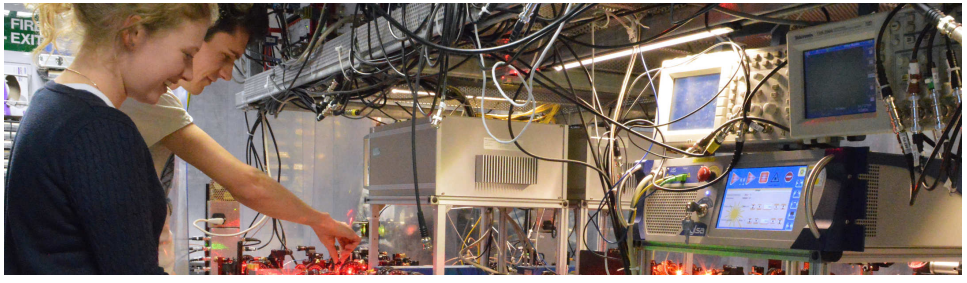
"trying to find a computer simulation of physics seems to me to be an excellent program to follow out (...) nature is not classical, dammit, and if you want to make a simulation of nature, you would better make it quantum mechanical, and by golly it is a wonderful problem, because it does not look so easy"

- Information processing based on quantum physics:
  Quantum Information Science

Imperial College London

Quantum Technologies: Hardware

- Build well-controlled quantum systems: approaches range from cavity quantum electrodynamics, optical lattices, ion traps, superconductors, quantum dots, linear optics, nuclear magnetic resonance, etc.



Imperial Centre for Quantum Engineering, Science and Technology (QuEST)

Hardware based (direct) applications

Quantum sensing, quantum clocks, quantum annealing, analogue quantum simulations, etc.

- Fully programmable quantum computer requires: Quantum Software

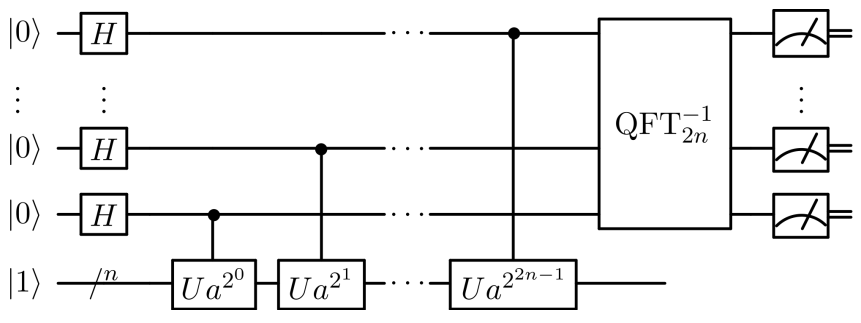
Imperial College London

Quantum Technologies: Software for Computation

Main motivation

We can do things that we do not know how to do using only (future) classical technology.

1. Quantum simulation of reactions in computational quantum chemistry for, e.g., the design of improved catalysts
2. Quantum computation with super-polynomial speed-ups over classical algorithms, e.g., solving certain linear and convex *optimization problems* or finding the *prime factorization* of large numbers



Shor's algorithm for prime factorization '94

(Wikimedia commons)

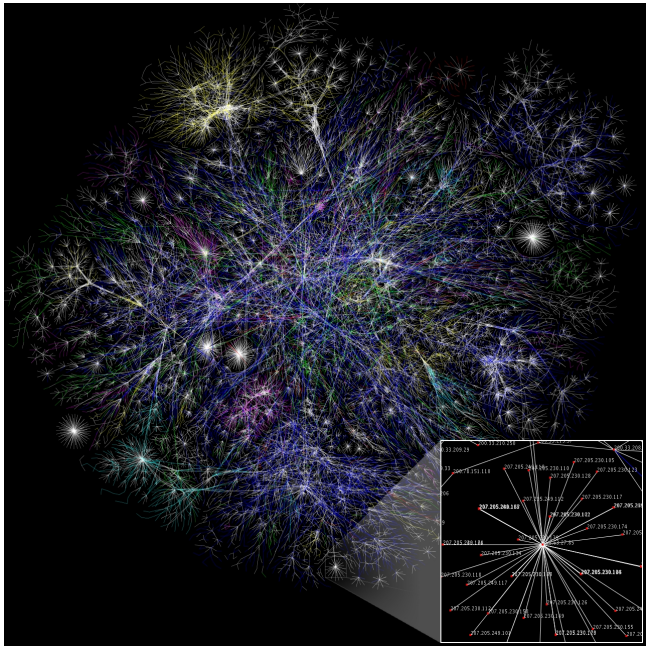
Quantum algorithm

for prime factorization breaks RSA public key cryptosystem – that is, virtually any encryption scheme in use today!

Imperial College London

Quantum Technologies: Software for Communication

3. Quantum cryptography has two aspects:
   - *Quantum-safe cryptography* studies how to protect from adversaries with access to quantum technologies
   - *Quantum-based cryptography* leading to, e.g., unconditional secure key distribution based solely on the laws of physics
4. Quantum communication using quantum repeaters for networks leading to the *quantum internet*



Graphical depiction of network
(The Opte Project)

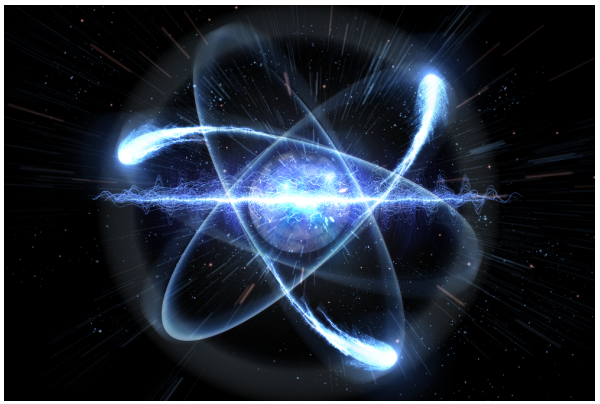
Our work

Mathematical aspects of quantum cryptography & quantum communication

Imperial College London

Quantum Technologies: Time to act

- Academic interest and funding:
  UK national network of quantum technology hubs (UKNQT) + EU quantum manifesto flagship-scale initiative in quantum technology
- Central intelligence agencies (GCHQ + NSA):
  "we must act now against the quantum computing threat in cryptography"
- Big private money for quantum technologies:
  Alibaba, Google, IBM, Intel, Microsoft, to name a few
- Explosion of start-ups



Quantum Technologies @Imperial

Thank you for your attention, Q&A time.