★ Quantum computing is the holy grail for computing research but is fraught with challenges. However, there is optimism and an encouraging degree of success, as **Tommaso Calarco**, **Philippe Grangier**, **Andreas Wallraff**, **Peter Zoller** and **Daniele Binosi**, from the QUROPE project discuss

Small steps that will lead to Quantum leaps

The history of quantum mechanics is a history of revolutions. Scientifically, its discovery represented a radical paradigm shift with respect to contemporary physical theories. Technologically, its applications deeply affected everyday life. Some of the most far-reaching applications – such as the transistor and the laser – are the building blocks of current electronics and telecommunications, and have heralded the birth of information society as we know it today. Yet, they merely act as a support for a completely classical mode of processing information, where logical degrees of freedom exhibit no quantum behaviour whatsoever. The realisation of this fact led at the beginning of the 1980s to speculations about the possible use of quantum-physical systems to perform calculations of complexity unattainable by systems behaving classically. Around that time, coming from a completely different corner, several researchers were already investigating fundamentally counterintuitive aspects of the theory, like the superposition principle exemplified in the Schrödinger cat paradox and the 'spooky action at a distance' resulting from quantum entanglement.

Two theoretical breakthroughs turned these first, rather foundational inquiries into application-oriented research: the quantum key distribution (QKD) protocol of Gilles Brassard and Charles Bennett, presented in 1984, and Peter Shor's quantum factorisation algorithm from 1994. Shor's algorithm is a method for decomposing a number into prime factors in a time exponentially shorter than any known classical algorithm would take and, as such, provides a possible route to breaking many of the currently used cryptographic codes. The 'BB84' QKD protocol, on the other hand, provides – somewhat ironically – a way to transmit a secret message with absolute security, even against 'eavesdropping attacks' carried out with a quantum computer.

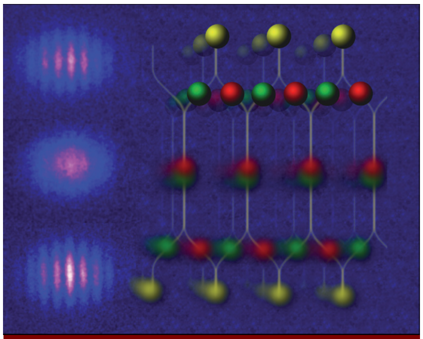


Illustration of the parallel entanglement of a very large number of atomic qubits, by using controlled cold collisions in an optical lattice (courtesy Immanuel Bloch, University of Mainz)

Both methods rely essentially on the ability to preserve and coherently manipulate superpositions of quantum states. This is relatively easy to achieve for quantum information encoded in photons propagating in free space or in optical fibres. Therefore, QKD – popularised as 'quantum cryptography' – has been developing quite successfully in recent years. But ultimately, for large bit rates or large distances (that is, more than about 100 km), noise and loss in photonic channels prevent secret bit transmission in practice. This limitation was lifted, in theory, about 10 years ago by introducing 'quantum repeaters'. These are, in essence, error-correcting devices that counteract the effect of the 'environment' on the qubits (such perturbations are unavoidable because no quantum system can be completely isolated from its surroundings). In the more general context of quantum computation, quantum error-correction codes theoretically allow for arbitrary quantum computations to be performed even with faulty gate operations, provided the error probability per gate is sufficiently small.

Quantum conundrums

While solutions to attain the ultimate goals – that is, unconditionally secure communication and devices that deliver immense computational power – do exist on paper, the limiting factor for their actual implementation is that for arbitrarily scaling up the number of qubits in a quantum computer, or the distance covered by a quantum communication channel, the initial 'uncorrected' error rates have to be already quite small. Unfortunately, the required values are not yet attainable practically. Several schemes for high-quality quantum gates have been put forward, starting with the ion-trap quantum computer proposed in 1995 by Ignacio Cirac and Peter Zoller. An increasing number of groups are trying to implement quantum gates with different experimental systems.

In order to get a clearer view of the state-of-the-art of the current available systems for quantum information processing and communication (QIPC) and the challenges that have to be overcome on the way to its practical realisation, 'roadmaps' have been put in place on both sides of the Atlantic. One of the most important activities carried out by the coordination action QUROPE, supported by the European Commission's Future and Emerging Technologies Unit, is thus the constant update and development of the 'Quantum Information Processing and Communication Strategic Report', also known as the 'European QIPC roadmap'.

The platforms for QIP

According to this roadmap, the platforms for QIP fall roughly into two major categories: atomic, molecular and optical (AMO) systems, and solid-state systems.

In the first category, the brightest candidates identified so far are trapped ions, and atoms confined in optical lattices. Systems based on trapped ions lead the race with respect to controlling individually a few qubits (up to eight qubits, a 'quantum byte'), whereas atoms in optical lattices provide a very large number of qubits in parallel, amenable to pair-wise interactions (individual addressability being the next challenge in this case). There are many other contenders, including photons within the 'linear quantum computing' approach, miniature traps for atoms or ions (known as atom chips or ion chips), as well as 'continuous variables' systems, where the usual qubit-based approach is replaced by continuous degrees of freedom, such as the amplitude of the quantised electric field, or collective spin in atomic ensembles.

Though there is clearly a long way to go, the recent successes outlined in the European roadmap justify an optimistic outlook on the future of QIP

There was recently significant progress in the second category, due to careful device design and material choice, which have enabled the storage and manipulation of quantum information in solid state architectures realised in super- or semiconductor micro- and nanoelectronic circuits, where two-qubit gates have also been realised. Moreover, inspired by atomic physics and quantum optics, cavity quantum electrodynamics ideas are now harnessed in solid-state systems to realise controllable coherent coupling between electronic qubits and individual photons. This approach is promising for achieving truly scalable architectures and as an interface for novel hybrid QIP systems.

Quantum communications

Within the vast range of QIPC activities, quantum communications and especially quantum cryptography are currently the most advanced ones, as far as applications are concerned. Several small companies worldwide are now selling QKD devices that yield decent data rates over distances of several tens of kilometres, and can be deployed in real case situations. For example, they have been used to protect a federal election that took place in the State of Geneva on 21 October 2007 against hacking or accidental data corruption in transmitting the electors' votes. Moreover an Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) has been created with the objective of bringing together the important European actors from science and industry (many large companies with an interest in telecommunication or information technology sustain an internal research programme on the subject), and start to address standardisation issues in quantum cryptography, and quantum technology in general.

Though there is clearly a long way to go, and no 'working quantum computer' yet, the recent successes outlined in the European roadmap justify an optimistic outlook on the future of QIP, not least in the face of the high expectations for applications that become possible once the technology has matured. The pace with which progress has been made, on both the theoretical and the experimental side, could not have been envisioned ten years ago. The major issues are well-identified, and all the first obstacles along the way towards practical working devices have been overcome, with controlled interactions and entanglement – required for scalable quantum computing – demonstrated with a number of physical systems. Also, there is a general consensus about the most important achievements so far, and the ways that should be taken, testified by strategic documents as the one described. Overall, research is progressing and becoming increasingly focused, with no signs of stagnation. Maybe the most difficult aspect to explain to outsiders – and 'deciders' – is that coping with the laws of nature has never been easy. Every step takes serious effort. And therefore, only long-term commitment will be successful. ★

At a glance

Full Project Title

QUROPE (Quantum Information Processing and Communication in Europe)

Project Objectives

- Unify, structure and strengthen the QIPC scientific community in Europe
- Develop a common strategy, vision and goals
- Congregate and coordinate all QIPC projects/actions at the EU level
- Support integration and cross-fertilisation across disciplines
- Extend investigations towards emerging new areas, topics and applications
- Encourage promising young researchers
- Increase the general public awareness and visibility of QIPC in Europe
- Establish international cooperation

Further information

For more information see:

T Calarco, P Grangier, A Wallraff and P Zoller, Nature Physics 4, January 2008.

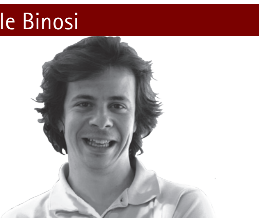
The QIPC Strategic Report can also be downloaded from:

W: www.qurope.net/Q_Reports/q_reports.php?type=reports&trig_id=1

Contact Details

Prof. Eugene S. Polzik, QUROPE Coordinator.
Niels Bohr Institute, QUANTOP - Danish Centre for Quantum Optics, Blegdamsvej 17, 2100 Copenhagen
W: www.qurope.net

Daniele Binosi



Researcher at the European Centre for Theoretical Studies

Daniele Binosi is a researcher at the European Centre for Theoretical Studies in Nuclear Physics and Related Areas in Trento. He leads QUROPE Workpackage 4.