

The second quantum revolution...

...leads to a second information revolution...

Quantum Information Science (QIS) has successfully combined quantum physics with information science, creating a new and unprecedented means for communicating and computing. Quantum Information Processing and Communication (QIPC) has the potential to become the basis for a second information revolution.

Historic development

In the late 1980s and early 1990s, quantum physicists started to discover new means of communication and computing, much more powerful than their classical counterparts and based solely on fundamental quantum principles. Today, 'Quantum Information Processing and Communication' (QIPC) is one of the fastest growing fields of information science and Europe has become one of its major global key players. European research programmes have been involved in QIPC from its beginning and have been following the expansion of the field with increasing investment and sustained support.

The potential of QIPC was recognised very early by FET – the Future and Emerging Technologies part of the IST Research Programme of the European Commission. Its support, vision and pathfinding role was crucial for the development of QIPC in Europe. In the Fourth Framework Programme (FP4, 1995–1998), quantum research gradually evolved towards the objective of 'Quantum Information Processing'. In FP5 (1999–2002), FET launched QIPC as a Proactive Initiative (PI). There were two calls for proposals and 25 projects were launched with a total cost of €41m and EU funding of €31m. One of the projects (IST Qucomm: Long Distance Photonic Quantum Communication) was awarded the EC's 2004 Descartes Prize for research. QIPC is also funded via the FET Open Continuous Submission Scheme, which

supports long-term, risky and visionary research. In this case, the research area is not specified in advance and QIPC projects are competing with all other areas sponsored by FET. In FP5, 10 QIPC projects with a total cost of €7m and EU funding of €5.6m were launched via this scheme.

In FP6 (2003–2006), QIPC continued as a FET PI, with five large-scale projects (three Integrated Projects, two Coordination Actions) and a funding volume of €27m. In addition, eight QIPC projects were funded via FET Open with €14m. In all funded projects the European dimension is a clear added value. Together with an accent on integration across different disciplines and approaches, it is considered crucial for the further advancement of QIPC in Europe. Two main events, a 'cluster review' with a conference as well as the annual European QIPC workshop provide a European forum for interactions between the members of the projects and for cross-fertilisation of ideas.

In addition, some areas of quantum cryptography that are closer to applications, now make part of the strategic objective 'Towards a global dependability and security framework', where a large Integrated Project (SECOQC) is funded. The consortium consists of about 40 partners, including several large companies. The EC funding is of €11.35m. The project includes all prominent groups in Europe active in this field.

The field of QIPC has advanced enormously and expanded in recent years: some areas are reaching maturity and developing technologies, while new advanced and forward looking areas are rapidly developing at the frontier of science. On the other hand, research at EU level has been a crucial factor for the development and expansion of this field. It has created research collaborations at pan-European level that have become

major players worldwide. It is the very nature of QIPC research that is flourishing in the environment created by pan-European collaborations. In order for Europe to maintain its leadership, it will be important to identify new sources of funding beyond what is currently foreseen in FP7.

The QIPC Strategic Report

Until now, European scientific publication output and quality in QIPC has been on a par with the US, while other nations (including Australia, Canada, China and Japan) have been systematically ramping-up in QIS investments. To retain Europe's leading position, European researchers have established a common research strategy for QIPC that allows fostering European strength and competitiveness. In an impressive joint effort, 40 of the most prominent European scientists and research groups contributed and put together a QIPC Strategic Report. This Report contains a detailed technical assessment, a summary of long- and medium-term goals, an outline of visions and challenges for QIPC in Europe, and constitutes a good example of how European research can be adequately structured with appropriate help from respective EU programmes. It is published in electronic form at the IST-FET website (cordis.europa.eu/ist/fet/qipc.htm). It has been updated continuously since 2005 in the framework of the project ERA-Pilot QIST, which was initiated to structure the European Research Area (ERA) with respect to Quantum Information Science and Technology.

The QIPC Strategic Report is a unique document constituting the scientists' clear vision to build a coherent European Research Area for QIPC with lasting significant impact on modern information society, and outlining a strategy of how this can be achieved. It builds on a specific feature and strength

of European research, namely the broad range of activities and expertise that coherently links efforts from experimental realisation all the way to basic theoretical questions in quantum information science and quantum physics. It is also an important and up-to-date document for decision-makers that will allow them to exploit the full potential of European research and to withstand the challenges of the international competition.

The second quantum revolution

QIPC has three closely interconnected subdomains: Quantum Computing, Quantum Communication and Quantum Information Science. Each of them constitutes a fascinating field by itself, holding the promise and potential of revolutionising the corresponding classical technologies that we are so familiar with today. The first quantum revolution, the development of Quantum Mechanics at the beginning of the last century, has given us an understanding of the new rules that govern physical reality. Among other things, classical computers are based on these rules. The second quantum revolution that we are experiencing today exploits quantum superpositions and their most counterintuitive consequence: entanglement, which is the very basis of QIPC.

QIPC deals with 'quantum information', which is something very precise and well defined. The general idea is based on storing, processing and retrieving information using physical systems that are dominated by the laws of quantum physics. The unique power of quantum information over classical information comes from the direct use of the most basic features of quantum physics: quantum superpositions and quantum entanglement, which are both impossible classically, and are very different from just exploiting quantum effects. These ideas have already led to the conception of machines and devices that are able to perform tasks which could not be accomplished before.

One example of a device that can outperform classical computers using the quantum information principles is a quantum simulator. A quantum simulator consists of entangled atoms that interact with each other in ways

prescribed and engineered by a researcher. By 'dialling' a particular interaction type, the researcher can model new kinds of materials. Such a simulator is so powerful that already with 50 atoms it can model materials that cannot be modelled by the most powerful modern classical computers.

Another particularly relevant example is the decomposition of a number into prime factors. The security of today's bank transactions over the internet relies on the practical observation that it is hard to factor the product of two prime numbers back into the original primes. If these primes are both 1,024 bits long, it is estimated that the sun will burn out before today's most powerful computers can factor the number. This is not quite so for quantum computers: they would solve the problem in a few hours, disclosing our data to potentially malicious eavesdroppers. On the other hand, quantum cryptography already provides the technology for achieving (through quantum encryption schemes) absolute secure communications over a few tens of kilometres. The data contained in a quantum encrypted message cannot be read by eavesdroppers even if they are equipped with a quantum computer.

There is a fascinating context of QIPC, broader than illustrated by the examples above, which consists in the integration of a wide spectrum of scientific fields both in theoretical and experimental physics, as well as from other disciplines like computer science, mathematics, material science and several areas in engineering. The European vision is to advance quantum information processing in such a wider context, which includes the spectrum from fundamental quantum physics to applications in science and engineering. To remain competitive, Europe must nurture QIPC technology innovation from fundamental research, which requires the transition of basic research with its accompanying spin-off technologies, into more application-driven research, where inherently QIPC-based applications are researched and developed. An early example of such a QIPC-driven application is quantum

cryptography with a number of Quantum Cryptography small and medium enterprises already in operation worldwide.

Quantum Information Technology is a fundamentally new way of harnessing nature and it has potential for truly revolutionary innovation. There is almost daily progress in developing promising technologies for realising quantum information processing, with various advantages over its classical counterparts. After all, the best way to predict the future is to create it. It might well be that the real computer age has not yet even begun.

For more information on QIPC projects, see cordis.europa.eu/ist/fet/qipc.htm or contact the QIPC FET Proactive Initiative Co-ordinator Antonella Karlson (Antonella.Karlson@ec.europa.eu).



Eugene Polzik
Professor of Experimental
Quantum Optics

Danish National Quantum Optics
Centre and Niels Bohr Institute
Blegdamsvej 17
DK-2100 Copenhagen
Denmark

polzik@nbi.dk
www.qurope.net

Anton Zeilinger
Professor of Physics

Faculty of Physics
University of Vienna
Boltzmannngasse 5
1090 Vienna
Austria

anton.zeilinger@univie.ac.at
www.quantum.at/zeilinger

Sir Peter Knight FRS
Principal of the Faculty of
Natural Sciences

Level 3, Faculty Building
Imperial College
London SW7 2AZ
UK

p.knight@imperial.ac.uk
www.imperial.ac.uk/naturalsciences