2. Introduction: The major vision and goals of QIPC

The theory of classical computation was laid down in the 1930s, was implemented within a decade, became commercial within another decade, and dominated the world's economy half a century later. However, the classical theory of computation is fundamentally inadequate. It cannot describe information processing in quantum systems such as atoms or molecules. Yet logic gates and wires are becoming smaller and soon they will be made out of only a handful of atoms. If this process is to continue in the future, new, quantum technology must replace or supplement what we have now. In addition, quantum information technology can support entirely new modes of information processing based on quantum principles. Its eventual impact may be as great as or greater than that of its classical predecessor.

While conventional computers perform calculations on fundamental pieces of information called bits, which can take the values 0 or 1, quantum computers use objects called quantum bits, or qubits, which can represent both 0 and 1 at the same time. This phenomenon is called quantum superposition. Such inherently quantum states can be prepared using, for example, electronic states of an atom, polarized states of a single photon, spin states of an atomic nucleus, electrodynamical states of a superconducting circuit, and many other physical systems. Similarly, registers made out of several qubits can simultaneously represent many numbers in quantum superpositions.

Quantum processors can then evolve initial superpositions of encoded numbers into different superpositions. During such an evolution, each number in the superposition is affected and the result is a massive parallel computation performed in a single component of quantum hardware. The laws of quantum mechanics then allow this information to be recombined in certain ways. For instance, quantum algorithms can turn a certain class of hard mathematical problems into easy ones – the factoring of large numbers being the most striking example so far. Another potential use is code-breaking, which has generated a great deal of interest among cryptologists and the data security industry.

In order to accomplish any of the above tasks, any classical computer has to repeat the same computation that many times or use that many discrete processors working in parallel. This has a decisive impact on the execution time and memory requirement. Thus quantum computer technology will be able to perform tasks utterly intractable on any conceivable non-quantum hardware.

Qubits can also become entangled. Quantum entanglement is a subtle non-local correlation between the parts of a quantum system. It has no classical analogue. An entangled state shared by two separated parties is a valuable resource for novel quantum communication protocols, including quantum cryptography, quantum teleportation and quantum dense coding. Quantum cryptography offers new methods of secure communication that are not threatened even by the power of quantum computers. Unlike all classical cryptography it relies on the laws of physics rather than on ensuring that successful eavesdropping would require excessive computational effort. Moreover, it is practical with current quantum technology - pilot applications are already commercially available.

While the central concepts of quantum information sciences have initially been developed for qubits, the alternative possibility to realize quantum informational and computational tasks using continuous variables has been investigated more recently. The use of quantum information carriers that have a continuous spectrum, such as the quadrature amplitudes of the quantized light field, has several potential advantages over qubit-based processes. Such advantages lie in the prospect for higher optical data rates and simpler processing tools, based upon standard telecommunication techniques. Another significant strength of this paradigm is that the light-atoms quantum interface can be designed for continuous variables, so that atomic continuous-variable systems can be used as a memory for light.

Experimental and theoretical research in quantum information science is attracting increasing attention from both academic researchers and industry worldwide. The knowledge that nature can be coherently controlled and manipulated at the quantum level is both a powerful stimulus and one of the greatest challenges facing experimental physics. Going to the moon is straightforward by comparison – though fortunately the exploration of quantum technology has many staging posts along the way, each of which will yield scientifically and technologically useful results.

In principle we know how to build a quantum computer: we start with simple quantum logic gates and connect them up into quantum networks. A quantum logic gate, like classical gates such as AND and OR, is a very simple computing device that performs one elementary quantum operation, usually on one or two qubits, in a given time. However, the more interacting qubits are involved, the harder it tends to be to engineer the interaction that would display the quantum behaviour. The more components there are, the more likely it is that quantum information will spread outside the quantum computer and be lost into the environment, thus spoiling the computation. This process is called decoherence. Thus the task is to engineer sub-microscopic systems in which qubits affect each other but not the environment. The good news is that it has been proved that if decoherence-induced errors are small (and satisfies certain other achievable conditions), they can be corrected faster than they occur, even if the error correction machinery itself is error-prone. The requirements for the physical implementation of quantum fault tolerance are, however, very stringent. We can either try to meet them directly by improving technology or go beyond the network model of computation and design new, inherently fault-tolerant, architectures for quantum computation. Both approaches are being pursued.

There are many useful tasks, such as quantum communication or cryptography, which involve only a few consecutive quantum computational steps. In such cases, the unwelcome effects of decoherence can be adequately diminished by improving technology and communication protocols. Here the research focus is on new photon sources, quantum repeaters and new detectors, which will allow long-distance entanglement manipulation and communication at high bit rates, both in optical fibers and free space.

Within a decade, it will be possible to place sources of entangled photons on satellites, which will allow global quantum communication, teleportation and perfectly secure cryptography. Quantum cryptography relies on quantum communication technology but its progress and future impact on secure communication will depend on new protocols such as, for example, quantum-cryptographic authentication and quantum digital signatures.

The next thing on the horizon is a quantum simulator. This is a quantum system in which the interactions between the particles could be engineered to simulate another complex system in an efficient way – a task that is inherently intractable on classical, but not quantum, technology. Building quantum simulators would allow, for example, the development of new materials, accurate description of chemical compounds and reactions, or a deeper understanding of high temperature superconductivity. The goal is to push the existing quantum technologies, such as optical lattices, to their limits and build quantum simulators within a decade or so.

Last but not least, the search for scalable quantum information technologies goes on. This astonishing field appears to involve practically the whole of physics, and stretches the theoretical and experimental resources of every branch of physics, from quantum optics and atomic physics to solid state devices. It is likely that there will not be a single winner in this search: a number of different technologies will complement each other. Some of them will be more suitable for quantum memories, some of them for quantum processing, some for quantum communication and so on. Therefore, in addition to developing individual technologies, we also need interfaces between these technologies, so that we can transfer a qubit, for example, from a polarized photon to an electron in a quantum dot. The hybrid technologies and architectures for quantum computation, including interfaces between them, are the long-term goals for years to come.

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. From the perspective of the future, it may well be that the real computer age has not yet even begun.

Source URL: http://qurope.eu/content/2-introduction-major-vision-and-goals-qipc