Quantum information processing and communication basics

Quantum Information Processing and Communication (QIPC) is a very modern and exciting field of research. It has nevertheless deep roots and has been long in coming: Its beginning can probably best be tagged on the famous Einstein-Podolski-Rosen paper in 1935 continuing with the work of John Bell in the 1960s and the findings of Alain Aspect in the 1980s. The quantum mechanical description of a regular Turing machine was given by Paul Benihoff in 1980 building on earlier ideas of Charles Bennett.

But it was really Richard Feynman, who first realised the superiority of quantum mechanical systems and showed in 1982 that a classical Turing machine would experience an exponential slowdown in the simulation of certain quantum systems. He found that a universal quantum simulator - itself being built on quantum processes - would not suffer from such shortcomings. The first quantum Turing machine was subsequently described by David Deutsch in 1985.

A first real breakthrough in the field came in 1994, when Peter Shor showed that the factorisation of prime numbers could be carried out on a quantum computer in a much shorter time than on a classical computer. This success triggered a flurry of work - still continuing today - both on the theoretical side but also on quite a number of potential technical realisations of quantum computers - receiving itself a boost from advances in nanotechnology.

With respect to quantum communication and quantum cryptography it may be noted that in a somewhat independent development already in 1970 a new cryptographic method was devised by Stephen Wiesner. In contrast to all hitherto existing methods it did not rely on mathematical transformations but used fundamental physical principles instead. A first experimental implementation of this idea was published by Charles Bennett and Gill Brassard in 1989.

Since then a number of remarkable advances have been realised and much more will be coming in the short-, mid- and long-term.

Source URL: http://qurope.eu/qipc/basics