

Short History of Quantum Information Processing

1. Implications of Quantum Physics

Civilisation has advanced as people discovered new ways of exploiting various physical resources such as materials, forces and energies. The twentieth century has added information. Computers allow complex information processing to be performed outside the human brain for the first time. The history of information technology has moved from one realisation to another with increasing speed: from gears to relays, to valves to transistors to integrated circuits. Now Quantum Information Processing has reached the stage where one bit of information can be encoded in quantum systems, for example, by using two different polarisations of light or two different states of an atom.

Early in the twentieth century physicists began to explore the behaviour of matter below the level of the atom. The first task is always measurement and early work centred on the smallest quantity of matter that could be identified: the smallest 'quanta' - hence 'quantum' physics. Rutherford split the atom and Alan Turing's work on Hilbert Space led him towards his definition of processing and the first thoughts on computing published in '*Computable numbers*' in 1936.

Early computers were constructed of gates and storage 'bits' made of many thousands of molecules. The components of today's processors are moving in the direction of a few hundred molecules. The computing industry has always known that miniaturisation would reach a barrier below which circuits could not be built, because their fundamental physical behaviour would change. These quantum effects were originally seen as a potential limit to future progress.

In 1935 Albert Einstein, Boris Podolski and Nathan Rosen proposed the famous paradox known as Einstein Podolski Rosen (EPR) entangled pairs. Namely, that interfering with the properties of one of a pair of entangled photons (the smallest measurable 'quanta' of light) would cause an instantaneous change in the properties of the other entangled photon, however far distant it was.

The potential of quantum physical properties are only just being realised. In 1982 Richard Feynman suggested individual quantum systems could be used for computation. In 1985 the Royal Society published a paper by David Deutsch at Oxford outlining the first description of a quantum

computer (Quantum Theory, the Church-Turing Principle and the Universal Computer). Instead of quantum effects being a barrier to computing he described how they could be seen as a great opportunity to take computing forward into a new era of speed and power. Gradually researchers began to study these possibilities, often in the face of derision and opposition from the established experts.

It is now expected that quantum physics will play a revolutionary role in the next era of computing, information processing and measurement. Over seventy institutions all over the world are working on a wide variety of application areas including processing units, logic gates and quantum bits (qubits); storage media; transmission systems and communications algorithms; distance, temperature and weight measurement; timing devices and quantum clocks. Transportation (quantum teleportation) may be far in the future, but we now know that “*beaming up Scotty*” is no longer entirely science fiction.

This report is primarily about quantum cryptography but it is important to put this in the context of the wider quantum developments. Quantum Cryptography is not some isolated concept but an integral part of a whole new paradigm derived from the fundamental laws of physics.

2. Quantum Cryptography.

In 1984 C H Bennett and G Brassard of IBM proposed the BB84 protocol as a means of using quantum effects for cryptography. This stimulated a number of initiatives. Then in 1991 Artur Ekert proposed using Bell - EPR pairs to encrypt keys. By 1998 Nicholas Gisin at the University at Geneva was able to demonstrate the polarisation encoding system of photons over cables running under Lac Léman. In 2002 the university set up a company to start to market a commercial version of this system. The Royal Radar Establishment at Malvern, now part of QinetiQ Limited, carried out some of the earliest work on EPR entangled photons and by 1999 was able to demonstrate a laboratory system using laser beams. Funding was then largely discontinued and the team dispersed. In 1999 Los Alamos National Laboratory published their work targeting ‘free air’ communications using satellites to provide global coverage in due course.

Subsequently at least thirteen organisations world wide have claimed to be able to demonstrate these phenomena, either through cable or by ‘free air’ line of sight.

In Austria a group is working on building a cable network and recently announced to have successfully transmitted funds across Vienna 'protected by entangled photons'. BBN Technologies of Boston Mass. has a DARPA research contract to develop systems, which can make use of the substantial quantity of installed dark cable. The government of Singapore is working on building a 'free air' backbone network for their city.

3. Quantum Computation

Four key events demonstrate the potential impact of quantum computation on classical cryptography i.e. the systems on which current communications depend.

In 1993 Peter Shor at AT&T Bell Labs published a quantum algorithm to factor large integers. A quantum co-processor could use this formula to factor a number of any size in a few seconds – this would compromise systems dependent on keys.

In 1997 Lov Grover at AT&T Bell Labs published a quantum algorithm for searching all the entries in a random database of any size in parallel - in effect instantly.

In 1998 David Cory, Neil Gershenfeld and Isaac Chuang used nuclear magnetic resonance to create a three qubit prototype quantum computer. Neil Gershenfeld claims that just 1,400 qubits could store the entire Oxford English Dictionary.

Marshall Stoneham of University College, London, has recently been awarded £3.7m by EPSRC to build a quantum computer by incorporating qubits into silicon chips, which could operate at room temperature. His target is to have a quantum co-processor by 2010.

The algorithms to destroy comprehensively the underlying architecture of existing communications security systems only await the successful implementation of a quantum co-processor. That this will happen is close to a certainty. When it will happen is unclear. Optimistic researchers forecast 2010, but the authors would not endorse this. When the final breakthrough does occur it could happen unexpectedly with little or no notice.

4. Teleportation and Measurement

For the sake of completeness it is worth noting that Anton Zeilinger demonstrated rudimentary teleportation in 1998 at his laboratory in Innsbruck University. A number of institutions in the USA led by JPL on behalf of NASA have demonstrated prototype quantum clocks and measuring devices. Colin Williams at Stanford forecasts that a quantum clock could multiply the capacity of conventional communications systems many times over.

5. Monitoring Developments

In 1986 Peter Marcer of CERN set up the Cybernetics Machine Specialist Group for the British Computer Society and has since organised a series of annual conferences in the UK.

In 1997 members of the Real Time Club in London proposed setting up a project to review the state of the art of quantum information processing, and as a result Brian Oakley set up the Quantum Computing in Europe Pathfinder Project for the Long Term Research Unit of the European Commission. This project culminated in a world conference in 1998 in Helsinki. The hundred or so delegates agreed upon the taxonomy of the whole range of quantum developments. This was used as the basis for a call for funding to the 5th Framework Research Programme of the EC.

In 1999 the European Institute of Quantum Computing was set up in London as a knowledge transfer network to continue the work of this European project team, but insufficient support was forthcoming and it was discontinued.

In the Spring of 2004 Professor Andrew Briggs, Professor of Nanomaterials at Oxford, and EPSRC Professorial Fellow announced the setting up of the Quantum Information Processing Interdisciplinary Research Collaboration (QIP IRC) to carry out basic collaborative research and bring academics and industry together.

There are a number of web sites world wide that list activities and conferences across the whole field of QIP, including a useful 'road-map' from Los Alamos. However, there is no source of independent, edited comment and information in this whole developing field, either for the expert, the business executive or the interested lay-man.

6. Mathematicians, Computing and the Financial Community.

Cryptography is very important to the financial community and the City has a long history of using the latest technologies. Indeed, bankers and stockbrokers were some of the first organisations to use computing.

A proposal was put to Coutts & Co (bankers) to use a computer to maintain customer accounts as early as 1958. Barclays Bank installed an experimental Emidec 1100 computer in 1960 and in 1962 the Financial Times started to use a computer to calculate the daily stock market indices, some years before the Wall Street Journal computed the Dow Jones Index. The first on-line information and data processing system with terminals on bankers and brokers desks and providing instant share prices and information was launched in London in 1966, some six months ahead of Wall Street.

Academics have also played an important role and have provided services to financial institutions on game theory and implemented various systems to track share, currency and commodity price movements and have suggested using quantum effects to underpin new forms of financial instruments, identify patterns for 'chartists' and even to create a new form of money. One of the leading academic experts in quantum cryptography spent many years after graduating working for a major financial institution.