Quantum Computer

Ever since Charles Babbage's conceptual, unrealised Analytical Engine in the 1830s, computer science has been trying very hard to race ahead of its time. Particularly over the last 75 years, there have been many astounding developments – the first electronic programmable computer, the first integrated circuit computer, the first microprocessor. But the next anticipated step may be the most revolutionary of all.

Quantum computing is the technology that many scientists, entrepreneurs and big businesses expect to provide a, well, quantum leap into the future. Quantum mechanics is a conceptually counterintuitive area of science that has baffled some of the finest minds – as Albert Einstein said "God does not play dice with the universe". The pace of technological advancement has remained relentless. Lately, the key to improving computer performance has been the reduction of size in the transistors used in modern processors. This continual reduction however, cannot continue for much longer. If the transistors become much smaller, the strange effects of quantum mechanics will begin to hinder their performance. It would therefore seem that these effects present a fundamental limit to our computer technology, or do they?

In 1982, the Nobel prize-winning physicist Richard Feynman thought up the idea of a 'quantum computer', a computer that uses the effects of quantum mechanics to its advantage .For some time, the notion of a quantum computer was primarily of theoretical interest only, but recent developments have bought the idea to everybody's attention. One such development was the invention of an algorithm to factor large numbers on a quantum computer, by Peter Shor (Bell Laboratories). By using this algorithm, a quantum computer would be able to crack codes much more quickly than any ordinary (or classical) computer could.

In the mysterious subatomic realm of quantum physics, particles can act like waves, so that they can be particle or wave or particle and wave. This is what's known in quantum mechanics as superposition. As a result of superposition a qubit can be a 0 or 1 or 0 and 1. That means it can perform two equations at the same time. Two qubits can perform four equations. And three qubits can perform eight, and so on in an exponential expansion. That leads to some inconceivably large numbers.

In fact a quantum computer capable of performing Shor's algorithm would be able to break current cryptography techniques in a matter of seconds. With the motivation provided by this algorithm, the topic of quantum computing has gathered momentum and researchers around the world are racing to be the first to create a practical quantum computer.