Physicists perform the first ever quantum calculation

11 December 2007

University of Queensland researchers are part of an international team to have made the first ever execution of a quantum calculation, a major step towards building the first quantum computers.

Professor Andrew White, from UQ's Centre for Quantum Computer Technology together with colleagues from the University of Toronto in Canada, said by manipulating quantum mechanically entangled photons – the fundamental particles of light – the prime factors of the number 15 were calculated.

“Prime numbers are divisible only by themselves and one, so the prime factors of 15 are three and five,” Professor White said.

“Although the answer to this problem could have been obtained much more quickly by querying a bright eight-year-old, as the number becomes bigger and bigger the problem becomes more and more difficult.

“What is difficult for your brain is also difficult for conventional computers. This is not just a problem of interest to pure mathematicians: the computational difficulty of factoring very large numbers forms the basis of widely used internet encryption systems.”

Ben Lanyon, UQ doctoral student and the research paper's first author, said calculating the prime factors of 15 was a crucial step towards calculating much larger numbers, which could be used to crack cryptographic codes that are unbreakable using conventional computers.

“Our goal is not to break these codes in practice, but to show that they can be broken, and motivate a move to a more secure system," Mr Lanyon said.

“These codes form the basis of most banking and computer security and has implications of how we keep all data secure in the future.”

Professor White said in any computer a problem must be broken down into manageable chunks.

“Classical computers use two-level systems called bits (binary digits) while quantum computers use two-level 'quantum-mechanical' systems called qubits (quantum bits),” he said.

“A qubit is like a coin that can be heads (on), tails (off) or simultaneously heads AND tails (on and off) or any possible combination in-between.

“This is impossible with normal bits but one qubit can be in two possible states, two qubits can be in four, three qubits in eight, and so on. Quantum memory sizes grow exponentially with the number of qubits.

“Functional large-scale quantum computers may be as many years away, and it is hard to know how they will change the world, but change our world they will.”

The research will be published in the prestigious *Physical Review Letters* later this month.

Source: University of Queensland