QUANTUM COMPUTING BREAKTHROUGH

Researchers from the **University of Queensland** collaborating with researchers at the **University of Illinois** in the US have reported successfully building and testing a C-NOT gate, an essential component to enable quantum computers to work. The gate was built using single particles of light, "photons".

Project team leader ***Dr Andrew White*** of UQ's School of Physical Sciences said that, in the every-day world, objects were either `here' or `there'. Currently computers were based on this premise, with bits that were either on or off.

However, in quantum mechanics objects can be in two places or 'states' at once, and quantum bits, or qubits, which carry information can simultaneously be on and off.

"The critical component necessary for a quantum computer to work is a Controlled-NOT (C-NOT) gate: a gate that lets one qubit control the state of another," Dr White said.

"If one qubit is simultaneously on and off, then both bits can become entangled that is, correlated in apparently impossible ways. It is entanglement that makes quantum computing so powerful."

In 1988 UQ's ***Professor Gerard Milburn*** published one of the first proposals for quantum computing. In 2001 Professor Milburn, in collaboration with co-workers ***Dr Manny Knill*** and ***Dr Raymond Laflamme***, then at Los Alamos National Laboratory, US, proposed a scheme to do quantum computing with light using only simple optical devices; so called "linear optics". A large number of groups worldwide have started major research programs to implement the proposal.

Until recently no-one had fully demonstrated a C-NOT gate. However, the researchers from The University of Queensland reported successfully building and fully testing a C-NOT gate.

At the annual review of quantum computing by the US Army Research Office (ARO), Dr White presented results from a C-NOT gate made using single photons the basic particles of light. The ARO sponsors the world's largest and most diverse research program in quantum computing, with over 89 groups in 11 countries working on a range of technologies.

In a world first, the UQ team demonstrated that their gate reliably makes one qubit control another. Using an automated tomography system developed in UQ's Quantum Technology Lab, Dr White reported that if one qubit is simultaneously on and off, the UQ gate produces highly entangled qubits.

The UQ team, which also includes ***Dr Jeremy O'Brien, Dr Geoff Pryde, Associate Professor Timothy Ralph*** (all from The University of Queensland) and ***Dr David Branning*** (University of Illinois), next plans to study gate errors. In a normal logic gate this is simple, as there are a small number of possible input states. It is more difficult in a quantum logic gate, as an infinite number of input states exist.The UQ members are a part of the **Australian Research Council Centre of Excellence in Quantum Computing Technology.** Their work has received US Army Research Office funding of US$0.75M for a three-year program.

DISTANCE CRITICAL CARE SYSTEM LAUNCHED

A Virtual Critical Care Unit (ViCCU) pilot project has been launched to provide a high-speed internet link between the **Blue Mountains District ANZAC Memorial Hospital and** Nepean Hospital.

ViCCU is a joint project between Wentworth Area Health Service and the CSIRO which will provide patients at Katoomba with long-distance, on-line, real-time critical care and access to specialists at the Nepean Hospital.

The Virtual Critical Care project uses second generation broadband Internet technology, developed by the CSIRO-led **Centre for Networking Technologies for the Information Economy** (CeNTIE), that delivers high definition video and sound in real time. It comprises a computer screen to monitor vital signs, two television monitors to display the patient and medical staff, a microphone and mobile cameras that can zoom in on crucial areas like wounds.

The network technology has been provided in collaboration with Argus Telecommunications, a division of the Rail Infrastructure Corporation, utilising spare capacity in the rail telecommunications infrastructure.

PROJECT TO DEVELOP MOBILE SECURITY SYSTEMS

A **Macquarie University** cyber security expert and communications technology company, QUALCOMM International, will investigate new communication security systems for the mobile environment with funding from an ARC Linkage-Projects grant.

The project, Algebraic Methods in Design and Analysis of Stream Ciphers, will be undertaken by ***Professor Josef Pieprzyk,*** Head of Macquarie's Department of Computing and Director of the Centre for Advanced Computing - Algorithms and Cryptography; ***Greg Rose,*** QUALCOMM's Vice President of Technology, and ***Dr Philip Hawkes,*** engineer.

The project will investigate the problem of communication security in the mobile environment where both confidentiality and authenticity are important. Stream ciphers are useful in this environment as they provide an efficient cryptographic protection using limited computing resources. Stream ciphers are symmetric encryption algorithms which can be designed to be much faster than any block cipher. While block ciphers operate on large blocks of data, stream ciphers typically operate on smaller units of plain text, usually bits. In contrast to block ciphers, stream ciphers keep some sort of memory, or state, as it processes the plaintext and uses this state as an input to the cipher algorithm.

"The project will create a platform for the Macquarie University scientists and the QUALCOMM experts to design new stream ciphers that are resistant against very powerful algebraic attacks," says Pieprzyk.

"We hope that this cooperative effort will add to the momentum gathering behind research into stream ciphers," adds Rose. "This should allow much