# Boffins seek quantum leap forward

A computer that uses DNA strands to solve complex mathematical problems.

Quantum computers which do the same job by capturing individual atoms and manipulating them with photons, or by blasting molecules with microwaves.

These were topics under discussion in Auckland last week at the first international conference models of computation.

"If 10 per cent of what we are discussing comes true, it will alter our lives enormously, from our daily lives to more serious and philosophical stuff, like should we change our understanding of the truth in mathematics," said conference chairman Christian Calude, professor of computer science at Auckland University.

Most of these computers are still at the theoretical stage. That means Auckland University's Centre for Discrete Mathematics and Theoretical Computer Science is able to make a contribution, without having to invest a lot of money.

"There have been specialised conferences on quantum computation and DNA computation. This is the first time the different groups have been brought together," Professor Calude said.

Silicon chips are becoming ever smaller and faster. Advanced lithography has given manufacturers the ability to print logic gates and wires fractions of a micron thick.

come, probably in the next two decades, when logic gates are made of only a handful of atoms.

"At some stage you will reach a level where classical mechanics no longer operate," Professor Calude said. "You are forced to go into quantum mechanics, because quantum mechanics operates at this small scale."

While the ideas behind quantum computing were raised in the early 80s by visionary physicist Richard Feynman and others, the field took off in 1994 when Peter Shor from AT&T's Bell Laboratories in New Jersey devised the first quantum algorithm that, in principle, can perform efficient factorisation.

The difficulty of factorisation, working out which prime numbers a number can be divided into, underpin encryption methods used to protect electronic bank accounts and other sensitive information.

> "The machine is nature itself. Computers are made by fools like me."

The idea of quantum computing became more then an academic curiosity as its potential for codebreaking became apparent.Re-search funding flooded into the field.

Seth Lloyd, a professor of mechanical engineering at MIT, said many of the tools for quantum computing came from known effects.
"The machine is nature itself. Computers are made by fools like me. All we are trying to do is use natural capacity to process information."

In a conventional computer, each bit of information is stored on the silicon as an electrical impulse, with a value of 0 or 1.

*NZ Herald, Wednesday, the 14th Februrary 1998*

A three bit computer can store one of eight values: 000,001,010 through to 111.
A calculation using those bits must be repeated eight times.

In a three bit quantum computer, each bit (or qubit) is on both state 0 and state 1 at the same time. A calculation need only be run once,a phenomenon known as parallel processing.

Professor Llyod has already created a three-bit device, using aniline in a test tube put under a nuclear magnetic resonance machine and subjected to microwaves. If quantum computers can be scaled up from the two and three bit experiments so far, extremely powerful computers can be made.

"A grain of salt has as many bits as the CPUs (central processing units) of all computers in the world."

DNA computing, which has similar characteristics to parallel processing, was born in 1994 when Leonard Adleman from the University of Southern California reported how he had used DNA in a test tube to solve a classical mathematical problem of how to organise a travelling salesperson's itinerary so the traveller can visit seven cities without passing through any city twice.

The problem was solved by cultivating DNA strands representing all possible answers, culling the wrong answers by a series of chemical reactions and analysing what was left.

Professor Llyod believes there is more potential for quantum computing than DNA computing, because the amount of extra DNA needed to solve larger problems increases exponentially.

But he said even if no one succeeds in making large-scale quantum computers, the research effort is greatly increasing, our understanding of the fundamental laws of nature.

*NZ Herald, Wednesday, the 14th Februrary 1998*