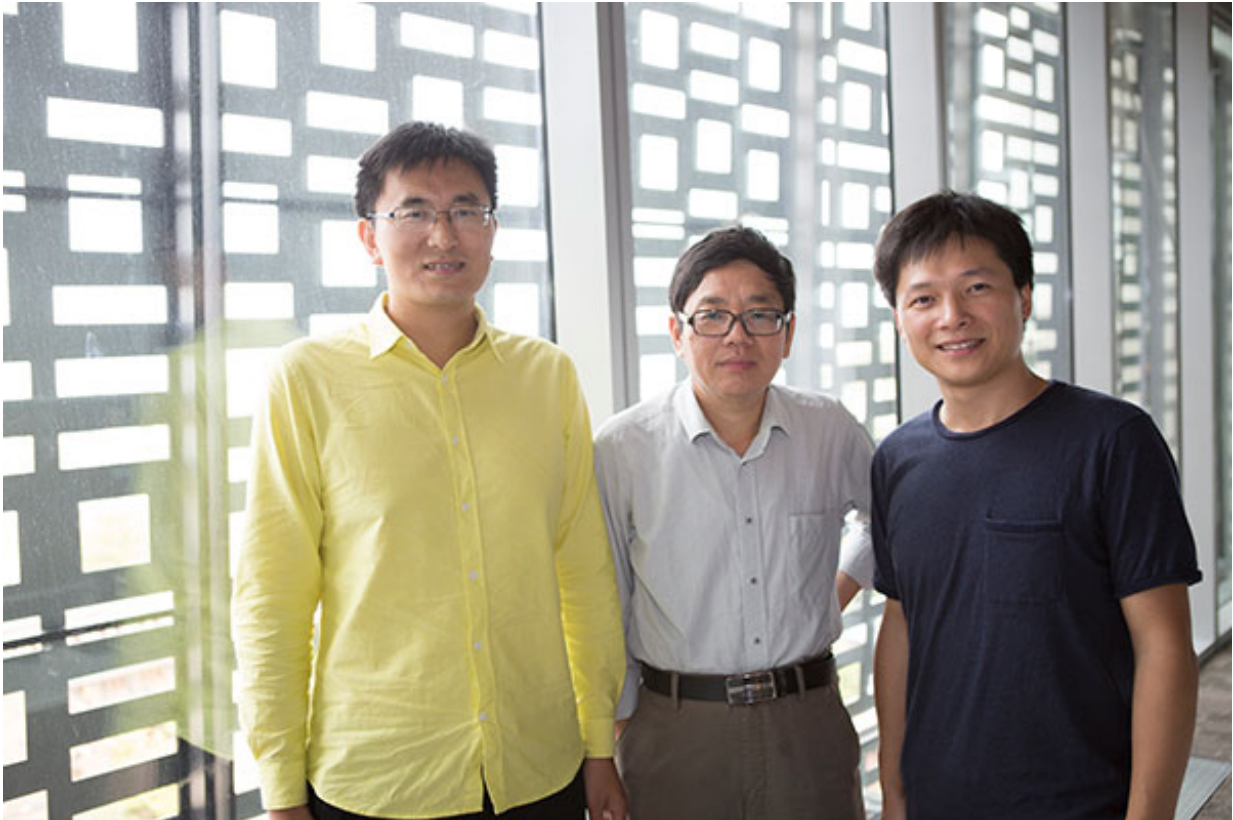# Quantum leaps

June 1 2015, by Elizabeth Kuo

Runyao Duan, Mingsheng Ying and Yuan Feng. Photo by Shane Lo.

Data may be king, but new research by the Centre for Quantum Computation and Intelligent Systems means we may soon see a coup. UTS's team of computer scientists are leading the development of a new pattern of programming language that will underpin how we use quantum computers and how we process data.

In today's deeply connected and informed society, data is everywhere. We collect digital information at an astounding rate, feeding data into enormous databases that monitor everything from genome sequencing, to astronomy and weather patterns, the rise and fall of global finance markets, even the social media accounts we manage on our hand-held smartphones.

Such technology enables society to accurately predict weather, prevent disease and manage consumer behaviour, but there are still many complex problems that cannot be solved by even the most advanced computers. And, as we continue to collect exponential amounts of data, this disconnect becomes even wider. Enter the world of the quantum computer – a new, and yet-to-be developed, computer that promises faster, more secure and more powerful processing, with problem-solving capabilities far greater than any classical computer.

A team of researchers from UTS's Centre for Quantum Computation and Intelligent Systems (QCIS) are at the forefront of developing a new pattern of programming language that will underpin how we use these quantum computers. They are Distinguished Professor Mingsheng Ying, and Professors Yuan Feng and Runyao Duan.

"The majority of research taking place in the quantum computing field at this moment is in building quantum computing hardware," says Ying. "But once a quantum computer is available and purchasable from the market, then quantum software will play a key role."

Ying says it's the first but most important piece of the puzzle. "We are focusing on the theoretical foundations for quantum software. Once these foundations have been laid, software can then be created and implemented, and following that, used by engineers to develop something practical for industry, consumers and society."

It only takes one look at the classical computer market, where the need for hardware pales in comparison to the multi-billion dollars generated by software sales, to understand how important this will be.

Laying the theoretical foundations for quantum computers is a sizeable research challenge, but Ying's research breakthrough – the establishment of a fully-fledged Floyd-Hoare logic for quantum programming – has assisted with bringing the team one step closer.

Floyd-Hoare logic was invented by computer scientists Robert Floyd and Tony Hoare in 1969. It describes the set of logical rules that underpin all of the computer programs being used today. Ying explains, "when you press the power button, hit the keyboard or run software updates on your computer, you are giving your computer a command. These commands rely on programs, or sets of instructions, to execute your task successfully.

"The Floyd-Hoare logic provides the basis of reasoning the correctness of these programs – to verify that your commands are executed exactly as you request it. This logic is the precursor to all classical computer programs in existence today."

Ying's adaptation of this logic to quantum programming has solved a notoriously difficult computer science problem – and signified a landmark achievement in the theory of quantum programming languages.

Building on the success of these findings, the team are pursuing research in other areas to better understand the possibilities of quantum computing. One of these areas is quantum entanglement, described by Duan as "one of the weirdest things to happen in quantum mechanics". Quantum entanglement is, by its simplest definition, a correlation between two systems, much stronger than any classical correlation.

Transcending the physical boundaries of time and space, its very weird nature is also what makes it so useful. Duan believes unlocking quantum entanglement will revolutionise the way we use next-generation information technologies.

"By exploiting the characteristics of quantum entanglement, we can create state-of-the-art techniques for super-reliable communication and build 100 per cent secure, unbreakable cryptographic systems. This will provide game-changing security technologies for banks, business, finance, police and counter-terrorism."

However, being able to quantify entanglement as a resource is not easy. "There are lots of technical challenges that occur in entanglement. It's fragile, it needs to be stored in very good quantum memory, and there's a lot of environmental noise to contend with," says Feng. "However, we realise the power of entanglement, and its potential real-world applications – and that's what motivates us to continue our research."

There is no doubt the work of Ying, Feng and Duan will prove to be powerful tools when large-scale quantum information processing becomes a reality – which leaves us to beg the question: how close are we to developing a quantum computer?

"That's a question you should ask a physicist, not a computer scientist!" Ying laughs. "While we are still at the very early stages of quantum computing, there is an international race led by companies such as Google, IBM and Microsoft, as well as research teams including the Australian Centre of Excellence for Quantum Computation & Communication Technology, to build a large-scale quantum computer. With their money and resources, the answer is hopefully soon.

"And this is crucial to us because without the hardware, it's very hard to see the impact of our work."