Fast and totally secure communication in quantum

November 7 2005

A new era of totally secure communication and information sharing is within reach, with physicists at ANU achieving possibly the world's fastest transmission of 'unhackable' data using bright lasers to generate an absolutely secret 'key'.

The breakthrough, in the field of quantum cryptography, would be of particular interest to defence and intelligence organisations, the government and finance industry, because it provides a method of communication between two parties that defeats eavesdropping and is far superior to current technology.

Where the security of conventional cryptographic methods relies on the complexity of mathematical operations, the security of quantum cryptography is guaranteed by the laws of physics.

Researchers of the Department of Physics in the Faculty of Science, led by Dr Ping Koy Lam, have developed an experimental prototype demonstrating this futuristic technology. They are currently investigating the commercialisation potential of the successful prototype.

The technology employs specially generated secret electronic data, or 'keys', to encrypt a message. Upon receipt of the encrypted message, the recipient uses a precisely matching decoding key to recover the original message. Only a receiver with an identical secret key can correctly decipher the encoded message. The information cannot be intercepted between these points.

The technology is based on a theory first proposed by Einstein and colleagues in 1935. They uncovered a peculiar phenomenon known as entanglement, which manifests itself at the quantum level in nature. It has since been assumed that entanglement was a key ingredient in implementing systems that harness this quantum effect. However producing entangled states requires specialised and expensive optical equipment.

To address this difficulty, an innovation by the ANU group works on an extension of the idea of entanglement, known as 'virtual entanglement'. This has resulted in a greatly simplified setup for the groups' experimental prototype.

There are two types of quantum cryptography: discrete systems, which transmit and measure characteristics of individual particles of light; and continuous variable systems, which operate with light beams, in a manner similar to conventional fibre optic communications systems. As the ANU experimental prototype employs the latter, it is far more compatible with existing telecommunication infrastructure.

"We understand we are one of the first groups using the bright lasers to have demonstrated the successful transmission of a secret key," PhD candidate Mr Andrew Lance said.

"Our recent paper describes the optics, electronics and algorithms we use to generate an absolutely secure key and extract it at the other end experimentally. We also believe it may be the fastest ever demonstration of quantum key distribution using continuous variables," PhD candidate Mr Vikram Sharma said.

"Governments around the world in particular are paying close attention to this research area — it has the potential to revolutionise information security in the way that the World Wide Web revolutionised the

availability of information," said research fellow Dr Thomas Symul.

The group's research has been published online in the international journal *Physical Review Letters*.

Source: Australian National University