Quantum decoys foil code-breaking attempts

19 July 2005

Laser-lit encryption key has immediate commercial applications

Computer code-makers may soon get the upper hand on code-breakers thanks to a new quantum cryptography method designed at the University of Toronto. Quantum cryptography uses particles of light to share secret encryption keys relayed through fibre-optic communications.

A paper published in the June 16 issue of the *Physical Review Letter* demonstrates how senders can vary the intensity of laser light particles (photons) used in fibre-optic communications to create decoys that catch eavesdropping attempts. “To exchange secret communication, the sender and the recipient first have to exchange a random series of 0s and 1s – known as the encryption key – through a sequence of photons,” says the study’s lead author Professor Hoi-Kwong Lo of U of T’s Department of Electrical and Computer Engineering and Department of Physics. The security of the message relies on the security of the encryption key. “If an eavesdropper tries to intercept the transmission of the encryption key, he will give himself away by disturbing the photons. However, real-life light sources occasionally send out more than one photon and an eavesdropper can steal the additional pulse without the sender knowing.”

To address this problem, Lo’s technique manipulates the laser to create different signals of various intensities that act as decoys to distract the eavesdropper from the secret message. “Any attack will necessarily affect the decoy states and therefore be caught by the legitimate users, who will then use an encryption key only when it is guaranteed to be secure,” says Lo, who adds that the work has immediate commercial applications.

The research was funded by the Canada Foundation for Innovation, Canadian Institute for Photonic Innovations, Canada Research Chairs program, Natural Sciences and Engineering Research Council of Canada, Ontario Innovation Trust and Premier’s Research Excellence Award.

Source: University of Toronto