Harnessing Quantum Phenomena for Secure Communication

Prof Christian Kurtsiefer

Department of Physics

Centre for Quantum Technologies

Traditional forms of communication rely on trust, but today there are many scenarios in which two parties who do not entirely trust each other need to exchange information in a secure manner. Two common examples of these two-party cryptographic problems are ATM withdrawals and secure auction bidding. A potential solution is a protocol known as ‘bit commitment’.

In collaboration with researchers from the School of Computing, Prof Christian Kurtsiefer and his team at the Centre for Quantum Technologies recently achieved a significant research breakthrough: the world’s first demonstration of secure bit commitment technology. The researchers showed that their bit commitment protocol is secure as long as one party’s quantum memory device is imperfect, an assumption called ‘the noisy-storage model’.

In the team’s proof-of-principle demonstration, they harnessed some of the strange phenomena of the quantum world to guarantee security, thereby eliminating the need for trust, at least theoretically. Their bit commitment protocol was executed experimentally by performing measurements on 250,000 polarisation-entangled photon pairs, demonstrating the feasibility of two-party protocols in the noisy-storage model using real-world quantum devices.

In addition to potentially facilitating secure bidding in auctions and safe identification in various transactions, this pioneering research also offers clues for implementation the technology in future devices. For example, hand-held quantum devices that use integrated optics to implement the photon exchange and measurement process may be just over the horizon.

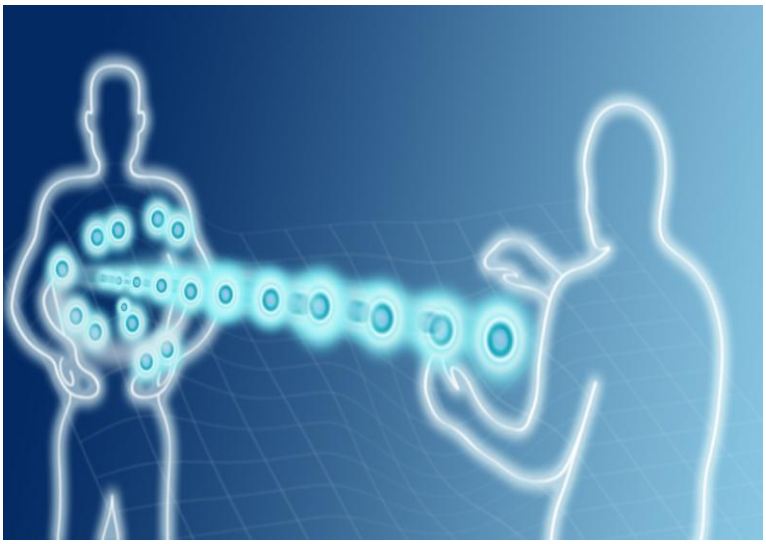

Figure 1. Artist's interpretation of two people communicating with quantum-entangled photons (credit: Timothy Yeo. Centre for Quantum Technologies).

Publication:

Ng, N.H.Y., Joshi, S.K., Chia, C.M., Kurtsiefer, C., and Wehner, S., Experimental implementation of bit commitment in the noisy-storage model. *Nature Communications* 3(1326), doi:10.1038/ncomms2268; arXiv:1205.3331 (2012).