Secure communication technology can conquer lack of trust

January 2 2013

Many scenarios in business and communication require that two parties share information without either being sure if they can trust the other. Examples include secure auctions and identification at ATM machines. Exploiting the strange properties of the quantum world could be the answer to dealing with such distrust: researchers at the Centre for Quantum Technologies (CQT) at the National University of Singapore have used the quantum properties of light to perform the world's first demonstration of a 'secure bit commitment' technology. The work is described in *Nature Communications*.

Secure bit commitment is equivalent to making a sealed bid in an auction. One party, usually known as Alice, 'commits' some information (a bit) to another party, usually known as Bob, with Alice later choosing when to reveal that bit. A bit commitment protocol is secure if Bob can't learn anything about the bit until Alice reveals it, and if Alice can't change the bit between committing and revealing it.

Compare this with a sealed-bid auction: the bidder must commit to an amount they will pay, and they should remain the only one who knows what the amount is until all the bids are revealed. This is desirable, because a dishonest auctioneer or anyone who accessed the information early could influence the bidding. At the same time, we want to make sure that the bidder cannot change the bid depending on any news he receives later on. This means that we cannot simply solve the problem by allowing the bidder to keep hold of their bid, because they might be dishonest and change the amount.

Traditional solutions to this problem – think sealed envelopes or data held by a third party – always depend on trust. Indeed, it has been proven that with classical information alone there is no solution that can totally protect the bidder and the bid receiver from unscrupulous behaviour.

In the demonstration, Alice communicates with Bob using photons, the particles of light. Alice creates pairs of photons that have the quantum property of being entangled, meaning that the photons' properties are connected even when they are separated. Alice splits each pair, keeping one photon and sending its entangled partner to Bob.

Alice encodes her 'bid' in her photons in such a way that Bob can only access the bid when Alice gives him instructions to decode his photons. But Bob can learn enough from his photons beforehand to know whether Alice is trying to cheat when she sends the instructions, say by using a different decoding. This way, both parties are protected from dishonesty.

The experiments were led by two Principal Investigators at CQT: Stephanie Wehner, who had earlier proposed a key theoretical requirement for secure bit commitment, and Christian Kurtsiefer, whose experimental group has expertise in creating entangled photons pair.

Wehner's idea was that secure bit commitment is possible with just one realistic, physical assumption: that anyone trying to cheat has limited ability to store quantum photons. (The quantum entanglement isn't enough on its own.) She proposed and developed this idea of 'noisy storage' in earlier papers.

"I wanted to demonstrate that secure bit commitment with the noisy storage model can work in the real world," says Wehner. With the experimental support from Kurtsiefer's group, it did. The team's Alice and Bob used 250,000 pairs of entangled photons to commit a bit secure against a memory of 972 quantum bits suffering a certain noise.

Quantum memories aren't even that big today, but if they got better, security could be restored by increasing the number of photons. The demonstration is a proof-of-principle that points towards a possible quantum technology for secure communication in our future.

More information: Huei Ying Nelly Ng et al, "Experimental implementation of bit commitment in the noisy-storage model", *Nature Communications* doi:10.1038/ncomms2268 (2012); preprint available at arXiv:1205.3331. www.nature.com/ncomms/journal/ … full/ncomms2268.html arxiv.org/abs/1205.3331

Provided by Centre for Quantum Technologies at the National University of Singapore