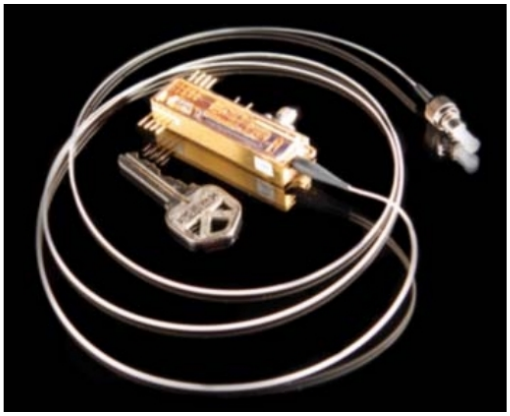
Written by Marco Attard
09 May 2013

The secretive Los Alamos National Laboratory claims it cracked the secret behind running quantum networks-- and doing it so successfully it has had a flexible quantum network running for 2.5 years.



Described as the secret sauce behind the ultimate in cryptography, quantum networking relies on the theory stating that the act of observing a quantum object (such as a photon) changes the object in question. This makes potential hackers detectable, and any cryptographic keys unusable.

The idea is hardly new. Commercial quantum cryptographic systems are already available from firms such as ID Quantique and MagiQ. However such systems can only send messages from A to B over a single cable, since the routing a message to locations C, D, or E involves some reading of the message, therefore changing it.

However the Los Alamos National Labs team has an alternative solution, one supposedly both easier and cheaper to implement-- network-centric quantum communications (NQC). Using a hub-and spoke approach, a central hub (dubbed "Trent") decodes an incoming message, transmits it to a new spoke, re-encodes it and fires it off.

Meanwhile the quantum cryptography transmitters (QKarDs) in use are relatively simple in design, being a random number generator and a laser inside a matchbox-sized unit.

"In our NQC test bed, which we have operated continuously for 2.5 years, we have time-multiplexed Trent with three QKarD transmitters, Alice, Bob and Charlie, over 50km of single-mode fiber; larger numbers of clients could be accommodated with a combination of temporal and wavelength multiplexing," the team writes in the paper "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection."

According to the team the system is scalable to up to 100 QKarDs (if using a PC) or around 1000 (via server), while the next generation of QKarDs should include Velocirandor, an improved random number generator capable of data rates of over 5Gbps.

There is one issue with such an approach-- the network is only as secure as the hub in the middle. In contrast, a "pure" quantum internet should allow secure communications from any part of the network to any other. Then again, the Los Alamos National Laboratory did manage to keep their quantum network a secret from the world for over 2 years, so who knows what it will reveal next?

Go Network-Centric Quantum Communications with Application to Critical Infrastructure Protection

Go Government Lab Reveals It Has Operated Quantum Internet for Over 2 Years (MIT Technology Review)