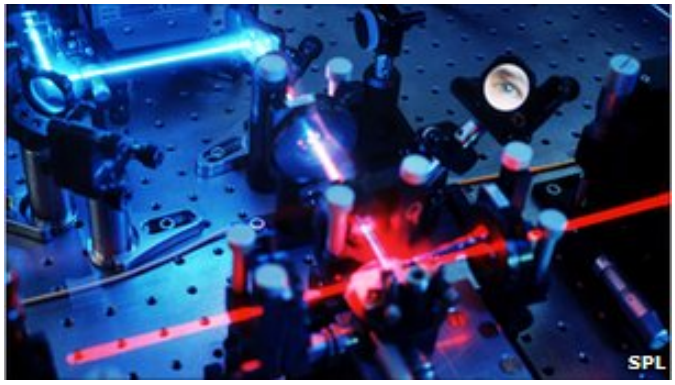
Written by Marco Attard
09 August 2012

Researchers based in Wuerzburg, Munich and Stuttgart discover a more efficient means of producing photons-- the single particles of light at the base of quantum computing, leading the way to potentially more practical quantum cryptography.



Quantum cryptography is incredibly secure. It uses a a quantum key distribution (QKD) link to share a secret encryption key (based in the polarisation of photons) between two computers. According to Heisenberg's uncertainty principle, one cannot listen to such communications without altering the polarisation, which results in detection.

QKD is already in use-- Switzerland used it to encode the 2007 national election ballot result. But current QKD production uses lasers to create photons, which can result in non-secure "multiple photon events."

The new method uses no lasers-- instead it involves 2 devices made of different semiconductor nanostructures. Each device emitting a single different-coloured photon when "excited" with an electrical pulse. Under laboratory conditions, a quantum key was created and successfully transmitted from sender to receiver across 40cm of distance.

According to the researchers the technology is electrically driven and compatible with standard semiconductor technology. It also can be (at least in theory) "very cheap."

But is quantum cryptography worth the research? Cryptography expert Bruce Schneier describes it as "unbelievably cool... and nearly useless in real life."

Then again, sometimes being really cool is enough right?

Go Major Step Taken Towards "Unbreakable" Message Exchange