

9 October 2008

By: Lucian Constantin, Web News Editor



Breakthrough in quantum cryptography bit rate  
PC Dynamics, Inc.

## [Quantum Cryptography Reaches Unprecedented Speed](#)

*Toshiba researchers have broken the 1 Mbps QKD transfer barrier for the first time*

The researchers from the Toshiba Cambridge Research Laboratory ([CRL](#)), have made a [breakthrough](#) in the Quantum Key Distribution (QKD) technology by boosting the secure key bit rates to over 1 Mbit/sec. This will make QKD networks 100-times faster than before as well as allow multiple network nodes.

Cryptography is based on the concept of sharing and comparing digital keys in order to verify authenticity of a connection, but the way in which the keys are normally distributed is not always secure possibly allowing for key theft. Protection from other techniques like crypto-analysis also implies changing the keys often. QKD is a technology that applies quantum physics principles to cryptography.

With QKD the key bits used for encoding are sent along the optical fibre in the form of single light particles (photons), which create patterns. The protection concept behind this is that an attempt at interception would disrupt the pattern thus messing the encoding and alerting the receiving devices. The special devices used to capture the single photons are called avalanche photodiodes and they allow electric circuits to detect the electron avalanches that occur when a photon is intercepted.

The problem lies with the fact that some trapped electrons can trigger a delayed echo, which can mislead the device into performing additional detections and corrupting the key. The solution is to temporarily stop the device after the initial detection in order to allow for the electrons to decay. However, this also translates into performance loss and low speed rates.

This only allowed quantum cryptography networks with a point to point architecture speeds of 10 kbps for 20 Km of fiber. The breakthrough consists of the discovery of a method that allows the detection of much weaker avalanches of electrons. Because the intensity is weaker, the probability of an electron becoming trapped is also significantly reduced, thus no longer requiring stopping the device. This in turn translates into greatly improved transfer rates as well as the possibility for the network to be split in up to 4 nodes.

Over 20 km of fibre, a raw bit rate of 9 Mbps can be achieved, which means a secure key transfer rate of over 1 Mbps. In comparison to the old technology, a 10 kbps speed now corresponds to a transfer over 100 km of optical fibre. The tests have been performed on a quantum cryptography network in Vienna, Austria.

"Together, the dramatic increase in bit rate and the possibility of network deployment, herald a breakthrough in the applicability of QKD technology. We plan now to develop a fully functional prototype of the high bit rate QKD system for use in quantum networks," said Dr Andrew Shields, head of the Quantum Information Group at CRL.