Video conferencing gets quantum security

Photon technology ramps up encryption speeds.

Quantum cryptography has been sped up to the point that it can be used to secure video conferencing.

Scientists from Toshiba's Cambridge Research Laboratory unveiled their invention to business leaders and government officials at Britain's Department of Trade and Industry in London on 27 April.

Their system is capable of generating 100 quantum 'keys' every second. This is fast enough for every individual frame of video to be protected by its own encryption. "This makes the system highly secure," says Andrew Shields, who leads the Cambridge team. "It would take an enormous computational resource to crack this frame by frame."

Toshiba representatives say the technology could be commercially available in as little as two years' time. Although it could initially cost up to US$20,000, Michael Pepper, managing director of Toshiba Research Europe Limited, says the price will plummet as demand increases.

Up to speed

Although video conferencing can already be secured using conventional encryption, this can still be intercepted and decoded by someone with sufficient computing power.

Quantum cryptography promises to stop such eavesdroppers. The system works by first establishing a 'key' that provides instructions on how to decode an incoming message. This key is built into the quantum state of photons. Intercepting a message breaks the key and alerts the sender and intended recipient to the security breach, because the very act of observing a quantum state changes it.

The Toshiba system creates keys made of 256 'bits', where each bit is a photon speeding along a fibre-optic cable. A photon represents either one or zero depending on whether it arrives slightly early or late at its destination. By passing a series of messages between the sender and receiver, both can arrive at a secure, mutually agreed key.

Once a key is established, a single frame of encrypted video signal is transmitted down a standard Ethernet cable. This process is repeated for every frame. The team hopes that in the near future, both keys and video will be able to travel down the same fibre-optic cable.

Unlike previous systems, which become unreliable when they heat up, this device can run continuously for more than four weeks, says Shields. The quantum information can only go so far before being corrupted by random interactions with surrounding material, however. "We've shown this can work over 120 kilometres of fibre," says Shields.

Quantum crackers

Experts are surprised by how quickly this technology has matured. "I did not really expect the thing to become practical, much less commercial, when I invented it with Charles Bennett back in 1984," says Gilles

Brassard of the University of Montreal, Canada. Brassard was part of the team that first demonstrated a working quantum cryptography device.

Brassard thinks that the main barrier to quantum encryption is demand. For most users, the nearly-uncrackable transmissions that are achieved through cheaper, simpler methods are good enough. "But the situation could change dramatically if quantum computers become a reality," he says.

Quantum computers are decades away from being built, but researchers believe they will boost computing power to levels that will enable codes to be broken very quickly.

"What most people don't realize is that classical encryption schemes can be broken retroactively," warns Brassard. "A spy can take down encrypted Internet traffic and set it aside until a quantum computer becomes available. I think quantum cryptography could boom when people realize this."