Unhackable telecom networks come a step closer

Chris Wickham, Reuters

(Reuters) - Researchers have come up with a way of protecting telecoms networks using quantum cryptography without the need for expensive dedicated optical fiber links.

The technique, developed by Toshiba's European research laboratory in Britain and Cambridge University engineers, is a step towards perfect security for everything from credit card transactions to private health records.

Quantum cryptography relies on the rules of quantum theory to generate uncrackable codes that encrypt data in a way that reveals if it has been eavesdropped or tampered with.

Governments and the military are thought to be using the technology already, based on systems available from firms like ID Quantique in Switzerland and U.S. rival MagiQ.

But until now, the quantum keys to encode and decode the information had to be sent on single photons, or particles of light, across a dedicated optical fiber separate from the line carrying the data itself.

"The requirement of separate fibers has greatly restricted the applications of quantum cryptography in the past, as unused fibers are not always available for sending the single photons, and even when they are, can be prohibitively expensive," said Andrew Shields from Toshiba Research in Cambridge.

"Now we have shown that the single photon and data signals can be sent using different wavelengths on the same fiber."

The Toshiba system, outlined in research published in the journal Physical Review X, still requires an advanced detector that picks up the encryption key in a time window of just 100 millionths of a micro-second, at the expected arrival time of the single photons.

But the detector, which is able to filter out the 'noise' in the fiber caused by the data itself, avoids the cost of laying down dedicated optical fiber lines.

Previous work has managed to use quantum cryptography on shared optical fibers but only over very short distances, with low capacity rates, or with data moving only in one direction.

The researchers say their system can do it over 50 km with data moving back and forth and an encryption capacity 50,000 times the record over the same distance.

Zhiliang Yuan [1], who worked on the research, told Reuters the team plan to carry out field tests on the system but he predicted it could be rolled out commercially within a few years.

(Editing by David Cowell)

Links:
[1] http://www.reuters.com/subjects/yuan