UK RESEARCHERS LEAD THE RACE TO DELIVER UNHACKABLE COMMUNICATIONS

Submitted by: Nelson Bostock Unlimited
Thursday, 5 June 2003

‘Unbreakable’ quantum cryptography demonstrated over fibre links longer than 100km for the first time
· Research led by Toshiba’s UK labs with further development to be funded by the DTI

June 5, 2003 - Cambridge, UK: Researchers at Toshiba Research Europe Limited (based in Cambridge, UK) have broken the distance record for the only unhackable form of communications called quantum cryptography.

The Toshiba research team is the first in the world to demonstrate successfully quantum cryptography over 100km of optical fibre, proving the broad commercial potential of the technology. Its achievement is being announced this week at the prestigious, global Conference on Lasers and Electro-Optics (CLEO) in Baltimore, USA.

Future development of the system will now be partially funded by the Department of Trade and Industry (DTI). The focus of the DTI initiative, which also involves the University of Cambridge and Imperial College, London, will be to realise a quantum cryptography system that is secure from every type of hacking.

Potential users of quantum cryptography include any organisation using IT and communications technology to send, receive and store sensitive information - from banks and retailers to central and local Government organisations.

Dr Andrew Shields, who leads the Toshiba group developing the system, said, "As far as we are aware, this is the first demonstration of quantum cryptography over fibres longer than 100km. These developments show that the technique could be deployed in a wide range of commercial situations within a timeframe of less than three years.”

“When more than 200 UK firms are targeted by hackers every day , delivering commercially available quantum cryptography will be a major weapon in the drive to ensure complete security for electronic communications," added Dr Shields.
Ian Williams, Programme Manager for the DTI's LINK Optical Systems Programme, which has supported this work said, “This is a substantial achievement by a world-leading UK team. It promises great improvements in IT security with potential benefits to IT users worldwide."

Cryptography, the science of information security, is essential to protect electronic business communication and e-commerce, enabling, for example, confidentiality, identification of users and validation of transactions. Much of the interest in quantum cryptography stems from the fact that it is fundamentally secure. This contrasts with today’s code based systems that rely on the assumed difficulty of certain mathematical operations. Ultimately, quantum cryptography seeks to deliver a method of communication whose secrecy does not depend upon any assumptions.

Quantum cryptography allows two users on an optical fibre network to form a shared key, the secrecy of

which can be guaranteed. This takes advantage of the particle-like nature of light. In quantum cryptography, each transmitted bit is encoded upon a single light particle (or 'photon'). The impossibility of faithfully copying this stream of encoded photons ensures that a hacker can never determine the key without leaving detectable traces of their intervention.

Until now, the major constraint on the appliance of quantum cryptography is that these light particles could be scattered out of the fibre. In theory, this is not critical as only the tiny fraction of photons that reach the other end are used to form the key. In practice, however, the rate of photons surviving long fibres can be so low that they are masked by the noise in the photon detector. By developing an ultra-low noise detector, the Toshiba team has been able to demonstrate a system working over much longer fibres than achieved previously.

Professor Michael Pepper, the Joint Managing Director of Toshiba Research Europe, commented, "The advance of semiconductor technology allows us to implement quantum effects which were previously thought to be only theory. One can foresee that this is the beginning of a process which will lead to a revolution in Information processing and transmission."

Further information please contact:

Dr Andrew Shields,
Toshiba Research Europe Ltd
260 Cambridge Science Park, Milton Road, Cambridge CB4 0WE, U.K.
Tel: 01223-436900
Fax: 01223-436909
e-mail: andrew.shields@crl.toshiba.co.uk

Rob Haslam or Caroline Howlett
Nelson Bostock Communications
Tel: 020 7229 4400
e-mail: rob.haslam@nelsonbostock.com or caroline.howlett@nelsonbostock.com