

State of the Art

1. Summary of Commercial Development

There is considerable activity worldwide in the area of QC both in commercial development and academic research and a number of international companies are selling or preparing to offer products for sale. This report details the published information, as well as noting potential activity which has not been published but alluded to through information garnered through research.

There are at least thirteen organisations who claim they have either products or who have developed prototypes which have been demonstrated to work in the laboratory, or are working on applications.

2. ID Quantique, Switzerland

Gregoire Ribordy
10 rue Cingria 1205 Geneva
Switzerland +41 022 702 69 29
Info@idquantique.com

IDQ was the first organisation publicly to offer a commercially available product in Spring of 2002. This company is a spin out of Geneva University and seeks to exploit the research of Professor Nicholas Gisin.

IDQ claims to have a Quantum Cryptographic product whose main features are: security guaranteed by quantum physics, encryption with AES or One-Time-Pad, transmission distance up to 100 km, automated key management, high transmission speed.

IDQ offers emitter and receiver units that can be connected to PC's through a USB port to transmit and receive point to point cryptographic keys through single uninterrupted glass fibre cable up to 70 km. Guide price €100k per system.

3. Cambridge Research Laboratory, Toshiba Research Europe

260 Cambridge Science Park
Cambridge CB4 0WE
Professor Michael Pepper FRS

Dr Andrew Shields
andrew.shields@crl.toshiba.co.uk

Are developing an off-the-shelf system which, unlike most of the other systems, implements quantum encoding, error correction and privacy amplification. They have reported the longest ever demonstration of full quantum key distribution over 122km. Also developing a fully quantum system based on a single photon light emitting diode which provides enhanced security and bit rates. Partially funded by DTI.

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 by 2006".

www.theregister.co.uk/20

4. MagiQ Corp. New York

Bob Gelfond

MagiQ QPN™ Security Gateway claims to be the first commercial implementation of Quantum Cryptography. MagiQ offers a commercial product, called Navajo, capable of transmitting a changing key sequence over a secure fibre-optic link of up to 50 kilometres as a stream of polarised photons. MagiQ claims they can change keys so frequently that the Advanced Encryption System (AES) could be made uncrackable. Systems have been installed on customer premises in the US.

Guide price \$50,000 - \$100,000 per set
www.magiqtech.com

5. NEC

Tim Rea.
NEC Europe, 1, Victoria Road
London W3 6BL
0208 752 3563
timothy.rea@ukneceur.com

NEC offers an advanced quantum key distribution system with planar light wave circuits at up to 150 km over public or private networks for projects

with special security requirements. The system is designed to transmit keys over a quantum channel (uninterrupted glass fibre cable) enabling the secure transmission of encrypted data over any public network.

“This system is enabled by a low noise photon receiver developed jointly by NEC and the Imai Quantum Computation Information Project in 2002 and a high performance transmitter developed by NEC and TAO that is equipped with a filter which can purify the single photon spectrum.”

www.nec.co.jp/press/en/0307/0401.html

6. BBN Technologies Cambridge Massachusetts: Boston University and Harvard University.

“This project, funded by Defence Advanced Research Projects Agency aims to develop a network of quantum links that can handle everyday applications like bank transactions. A six server network is operational using software controlled optical switches based on lithium niobate crystals. The longest link is 10 kilometres from BBN laboratories to Harvard University.”

[reported June 04]

<http://quantum.bbn.com>

7. IBM Yorktown.

Charles Bennett. Ralph Landauer.

IBM research laboratories carried out some of the original work on Quantum Information Processes and designed the two standard protocols known as BB84 and B92. Current work is being carried out in Zurich.

8. Hewlett Packard

Palo Alto and Bristol England are working with Neil Gershenfeld, Issac Chuang & Seth Lloyd of MIT on a \$25m five year Quantum Information systems project.

Stan Williams
Director of Quantum Science
Research
HP Labs, Palo Alto, California

9. University of Vienna.

Professor Anton Zeilinger

Universität Wien Institut für
Experimentalphysik
Andrea Aglibut +43 (0) 1 4277 51166
Andrea.aglibut@univie.ac.at
www.quantenkryptographie.at

Project funded by the European Union, University of Vienna together with the Austrian Research Center Seibersdorf and the Bank Austria Creditanstalt using cable laid by Wien Kanal Abwassertechnologien.

Has transmitted information along dedicated glass fibre cable over 1.45 km using entangled photons to provide ‘one time pad’ encryption of messages. Has also demonstrated free air transmissions with entangled photons across the Danube with a distance of about 600m.

10. Mitsubishi. Laboratories, Japan

A team is working on Quantum Information Processing Systems.
www.global.mitsubishielectric.com

11. The Singapore Government

The University of Singapore is installing a basic free air communication system in the City. This Research is being carried out through A-Star (Agency for Science, Technology and Research) and DSTA (Defence Science and Technology Agency) and is funded by the Singapore Government.

12. QinetiQ Ltd (Malvern UK).

Dr Brian Lowans
QinetiQ Malvern Technology Centre
St Andrews Road Malvern WR14 3PS
01684 543736
bslowans@qinetiq.com

QinetiQ performed some of the pioneering experiments in quantum cryptography in fibre, free-space (lasers) and entanglement. Currently developing a high-speed free-space QC system that can be installed quickly and easily to provide secure communication in city environments where

polarisation can be used to create keys that can be used in a ‘one time pad’ system to transmit information over conventional networks. Demonstrated distances of 24km and also currently developing satellite to ground applications.

13. Los Alamos

Free air (to, between and from satellites). Richard Hughes has been working on free air systems for some six years

14. National Institute for Standards and Technology in Boulder Colorado. (NIST).

High speed infrared laser systems capable of generating one million bits per second to protect applications such as video streaming. Free air system currently reported to be able to transmit over 700 metres.

15. Fujitsu

“Joint research project of Fujitsu Ltd and the University of Tokyo has made progress towards realizing a viable quantum cryptographic system”
www.infoworld.com

16. Other Relevant Research and Activities

Quantum Information Processing Interdisciplinary Research Collaboration (QIP IRC)

Director: Professor Andrew Briggs, Professor of Nanomaterials at Oxford, and EPSRC Professorial Fellow is carrying out basic collaborative research and bringing academics and industry together.

Quantum Relays.

The Jet Propulsion Laboratory (JPL) of the California Institute of Technology (Caltec) claim [*Physical Review A* Aug 2003.] to have devised a way to build a quantum repeater using ordinary optical equipment that

boosts the signal while preserving the entanglement of photons being transmitted.

The University of Geneva have made similar claims [*Physical Review Letters* Jan 2004]

Single Photon Sources

An Ultrabright Tunable Photon-pair source has been announced by MIT [American Institute of Physics *Bulletin of Physics News* 655 Sep 03]

Quantum Co-processor.

Marshall Stoneham of University College, London has recently been awarded £3.7m by EPSRC to build a Quantum Computer by incorporating qubits into silicon chips which could operate at room temperature. The target is to have a quantum co-processor by 2010.

Quantum Information Processing, generally

There appear to be over 60 Universities world-wide who have established Quantum Information Systems Research projects. There are frequent reports of researchers announcing working components for potential quantum processors.

Roadmap

A Quantum Information Science and Technology Roadmap has been published in the USA by the Los Alamos National Laboratory at:

<http://qist.lanl.gov>