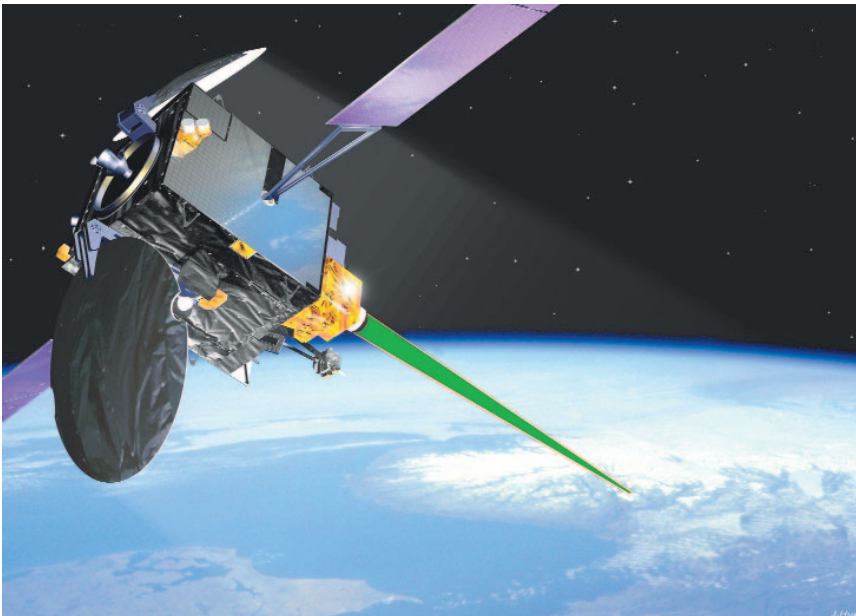


Quantum Cryptography



Global key management

- Unbreakable security
- Global capability
- Agile key distribution
- Automatic detection of eavesdroppers
- Low cost and rapidly deployable

Absolutely secure communications is now possible.

In a world of increasing reliance on electronic communications there is a need for high levels of trust and security. Applications range from electronic payment systems to military communications.

Current security relies on encryption through Public Key Infrastructure (PKI). The "master keys" are still distributed as physical tokens by couriers.

PKI may be broken by future cryptographic developments. This would mean that all past messages could be read. Physical key tokens carried by couriers could be compromised, which may not be detected.

There is a growing need for stronger security.

Quantum cryptography enables absolutely secure distribution of encryption keys. Communications protected by these keys can continue as normal through existing networks.

Quantum cryptography offers enhanced security with minimal changes to existing networks.

QinetiQ is developing a family of quantum cryptography based products.



Are couriers secure and cost effective?

Quantum Cryptography Capabilities

QinetiQ products based on quantum cryptography will enable

- automatic distribution of encryption keys with absolute security
- rapid generation of random numbers for use as session encryption keys or seeds for cryptographic algorithms
- the generation of large volume of keys.

These properties enable better key management techniques and strategies.

- Dynamic re-keying of session keys.
- "One-time pad". For the first time information management systems can provide the ultimate security.

QinetiQ Technologies



System transmitter

This is the first "through-the-air" system to offer full quantum cryptography security.

- Compact and portable.
- Unique synchronisation scheme for transmitter and receiver.
- Error correction.
- Privacy amplification to provide the final secure key.
- The system can be adapted to interface with different network architectures.

QinetiQ Solutions

Real-world applications for quantum cryptography will require a mix of free-space and fibre-optic solutions.

QinetiQ can develop a range of through-the-air and fibre-optic quantum cryptography systems tailored for particular customers or applications.

Applications

Quantum key transmission through-the-air has several important short range applications.

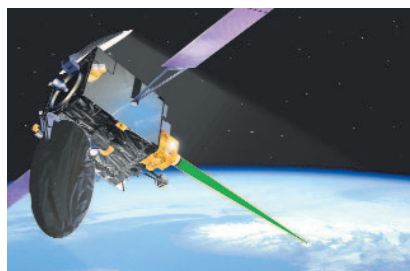
- Where businesses are not directly connected to each other by fibre.
- Urban environments and LANs where line-of-sight is possible.
- Remote or difficult environments.
- "Through-the-air" is a flexible solution and quick to install.
- Disaster recovery situations.



Quantum key transmission – "through-the-air"

Global Key Management

Fibre-optic based quantum cryptography systems are limited in range to 200km for the foreseeable future. For applications requiring connection over greater distances the only secure method will be quantum cryptography via satellite.



Global key distribution

Global optical communications using satellites has already been demonstrated by the European Space Agency (ESA). QinetiQ is at the forefront of developing quantum cryptography technologies for satellite based communications.

Key Milestones

QinetiQ has over 15 years experience in developing quantum cryptography technologies.

- 2005 – QinetiQ delivers world's first free-space quantum cryptography system to BBN. Designed as "plug & play" the system is successfully installed into the DARPA Quantum Network in USA.
- 2004 – QinetiQ shares the European Commission's prestigious Descartes Prize for quantum cryptography.
- 2002 – QinetiQ achieves current world record of 23.4km through the air for quantum cryptography.
- 2000 – QinetiQ demonstrates free space key transmission over 2km.
- 1993 – QinetiQ first to demonstrate quantum cryptography in fibre-optics.
- 1990 – QinetiQ first to demonstrate photon entanglement.



FS 73052

For more information please contact:

Customer Contact Team

QinetiQ

Cody Technology Park
Ively Road Farnborough
Hampshire GU14 0LX
United Kingdom
Tel +44 (0) 8700 100942
www.QinetiQ.com

Copyright © QinetiQ Ltd 2005
QinetiQ/S&DU/T&P/OPT/DS050074