

The Science & Potential of Quantum Cryptography

1. Issues with Classical Cryptography

Electronic commerce depends upon the existence of mechanisms for establishing trust between the parties concerned. The security mechanisms in use today rely upon classical cryptography:

- to verify the source of a message.
- to authenticate the receipt of a message.
- to demonstrate that it has not been tampered with.
- to prevent it from being read by anyone other than the intended recipient.

Classical cryptographic systems rely upon the use of a secret key, shared by the sender and recipient, which is used to encode and decode the message. Security depends upon this key not being available to any eavesdropper. So, before they can communicate securely, the sender (Alice) and recipient (Bob) must first find a secure way to share the secret key. This can either be done through some physical means – e.g. by courier – or by the use of a public key cryptographic system (PKCS), which requires each participant to have a pair of keys: one of these is a secret known only to them (private key), and the other can be publicly shared (public key).

Such systems are subject to a number of weaknesses.

- Physical transport of keys is slow, expensive and open to compromise.
- Key management, whether using PKCS or some other means, is expensive, cumbersome, and also open to compromise.
- The secrecy of the algorithms used depends upon the computational difficulty of factorising very large numbers. None of them is provably secure, and there is always the chance that someone might discover a way of breaking them. Moreover, when practical quantum computers are ever realised (see 3.1) they will be able to decode such messages by brute force.

- There is generally no way of telling that a key has been compromised or that a transmission has been intercepted. If thieves, hackers or terrorists were to get hold of a way of cracking these codes, they could covertly exploit their knowledge potentially disrupting financial markets and currencies and government.

Quantum Cryptography (QC) potentially offers a solution to all of these problems:

- Its security depends only upon the laws of quantum physics, and this is provably the case.
- It provides a mechanism for sharing secret keys that avoids both the administrative complexity and the vulnerabilities of other approaches.
- Uniquely, it provides a mechanism by which any attempt at eavesdropping can be detected immediately.

QC therefore, has the potential to offer improved security and operational benefits, as well as offering protection against threats to classical systems.

2. How it Works

Conventional data transmission uses electrical signals to represent a binary '1' or '0'. QC uses the polarisation, or phase states of individual photons of light to represent the binary digits.

Scientists claim that QC theoretically offers absolute security through the basic laws in quantum physics. Two approaches are possible. The first of these relies upon the 'uncertainty principle', which states that a single photon cannot be detected and its polarisation (or phase state) measured simultaneously. In other words the superposition of a pair of quantum 'observables' cannot be measured without interfering with the measurement of the other. Moreover, under the 'no cloning' theorem it is not possible to clone a photon so that one can be measured and the other passed on to the recipient. By the use of suitable protocols, involving additional communication over a conventional public communications channel, any attempt to intercept the data may therefore be detected. The first provably secure QC protocol, known as BB84, was proposed by C H Bennett and G Brassard of IBM, in 1984, and has been widely implemented.,

A different approach relies upon the Einstein, Podolski, Rosen (EPR) property of 'entanglement', which says that if two photons are in 'entangled' states, then any measurement of one will give a value that is directly related to the value of the other, irrespective of their physical separation. So if pairs of entangled photons are used to encode the data, and if one is transmitted to the recipient and the other retained by the originator, then again with suitable protocols, any attempt at eavesdropping may be measured by its impact upon the photons received. A QC protocol based upon EPR has been devised by Professor Artur Ekert of Cambridge University.

The former approach is easier to realise in practice and is used in most current implementations.

3. Current Implementations and Challenges

There are two methods of transmission. The photons used to encode data may be transmitted either through optical fibres or through free space, and both approaches have been demonstrated.

A serious challenge with either approach is that, in practice, a large proportion of the photons transmitted will be lost en route. This can be overcome to a degree by the use of appropriate error correction protocols and very low noise detectors. The protocols outlined above all have this capability, and systems have been demonstrated which are tolerant of path losses of 30dB – that is 999 of every 1000 photons is lost. At present transmission has been achieved through 120km of optical fibre and 23km in free space, but 150km in free space is expected soon. Transmission from low orbit satellites is expected to be possible within the next few years, and this would potentially allow world-wide communication, at least in circumstances where cloud cover is not too much of a problem.

Another significant challenge is that QC transmission is only possible on a point-to-point basis. Any form of switch, amplifier or relay destroys the quantum protection. However various ways of overcoming this are potentially possible including:

- optical switches which can redirect the photons without measuring them
- quantum relays based upon entanglement, which could in principle increase the distance possible through fibre

- conventional relays which are physically secured

These are all being actively developed, both in the USA and elsewhere. Using these techniques and ingenious software it is possible to build more complex networks, hub and spoke systems and long links which can be used in a limited number of early applications.

The transmission rates that can be achieved over QC links are comparatively slow. They are directly impacted by path losses, and so far throughputs of only a few kbits/sec have been demonstrated at the path lengths quoted above. Normally the QC link is used only for key distribution, and the encrypted data is transmitted over a conventional network, switched or otherwise, that does not need to be secure. For low volume transmission it is feasible to use key lengths as long as the data, in which case the encryption can use a one-time pad algorithm, which is completely secure. Otherwise conventional encryption algorithms such as Advanced Encryption Systems (AES) must be used, but it is feasible to change encryption keys completely securely at least ten times per second, which makes the task of any eavesdropper with access only to the encrypted data channel very hard indeed. Any attempt to intercept the key distribution process would of course be detected.

4. Conclusion

The QC mechanisms outlined above have all been demonstrated, and some thirteen organisations around the world claim to have developed working systems. In particular QinetiQ Ltd have demonstrated a free air system, and the Cambridge Research Laboratory of Toshiba Research Europe have demonstrated a cable-based system. So pilot applications should be practicable now.

However, quite apart from the limitations on range and connectivity already noted, there is significant work still to be done before this technology is likely to be widely deployed. This includes the more detailed specification and standardisation of all the communication protocols required and software integration with existing systems and infrastructure.

One object is to dispense with the problems associated with the management of the distribution and secure storage of keys and the associated costs. Protocols need to be devised so that the keys can be

integrated into the transmission algorithms. Further operating procedures will be needed to authenticate the bona fides of the receiver.

Commercial applications will require queuing systems, procedures to respond to denial of service, compliance with legal and accounting requirements and verifiable audit trails. Similarly, robust systems will need to be reconfigurable to meet changing circumstance and operational requirements, and the security of the immediate environs to terminals addressed.

All these will involve close working between developers, potential users of the technology, and the mainstream infrastructure suppliers.