

Introduction to Quantum Cryptography

Quantum Cryptography (QC) offers a secure method of sharing sequences of random numbers to be used as cryptographic keys. It can potentially eliminate many of the weaknesses of conventional methods of key distribution. Scientists claim that:

- The laws of quantum physics guarantee the security of sharing keys between two parties. The process cannot be compromised because information is encoded on single photons of light, which are indivisible and cannot be copied.
- Uniquely, it provides a mechanism by which any attempt at eavesdropping can be detected immediately.
- It provides a mechanism for sharing secret keys that avoids both the administrative complexity and the vulnerabilities of the other approaches.

QC has the potential to offer increased trust and significant short term operational benefits, as well as providing protection against threats which might be perceived as of a longer term nature.

Conventional data transmission uses electrical or optical signals to represent a binary '1' or '0'. These are sent as pulses through a transmission medium such as an electrical wire or a fibre-optic cable. Each pulse contains many millions of electrons or photons of light. It is possible therefore for an eavesdropper to pick off a small proportion of the signal and remain undetected. The eavesdropper can potentially gain information from the exchange of data in the PKI process or the subsequent symmetric encryption. Or the eavesdropper can pretend to be one of the parties.

QC is quite different because it encodes a single bit of information onto a single photon of light. The laws of quantum physics protect this information because:

- Heisenberg's Uncertainty Principle prevents anyone directly measuring the bit value without introducing errors that can be detected.

- A single photon is indivisible which means that an eavesdropper cannot split the quantum signal to make measurements covertly.
- The quantum ‘no-cloning’ theorem means that it is not possible to receive a single photon and copy it so that one could be allowed to pass and the other one measured.

A potential snag is that in real systems, not all the photons will be received, due to inherent losses in the transmission medium. A practical QC protocol needs to incorporate some method of determining which photons have been correctly received and also of detecting any attempt by an eavesdropper to sit in the middle of the channel and act as a relay.

The first provably secure protocol for QC that resolved these problems is known as BB84, and named after its inventors Bennett and Brassard in 1984. This protocol employs two stages

- Quantum key distribution (QKD), using an encoding which introduces a deliberate ambiguity by randomly changing between two different polarisation bases (either $0^\circ/90^\circ$ or $-45^\circ/45^\circ$) to represent a ‘1’ and a ‘0’ (i.e. four different polarisation states in all).
- A sifting process where the communicating parties use a normal communications link to confirm when each of these two bases was used.

Information theory can then be used to reduce the potential information obtained by an eavesdropper to any arbitrary level. Classical error correction algorithms calculate the error rate and remove these errors from the key sharing process. Security proofs have been developed to show that BB84 is absolutely secure provided that the error rate is kept below a specified level. A more detailed description of the BB84 protocol is given below.

There are several other protocols being developed

- B92 (invented by Bennett in 1992) used only two polarisation states 0° and 45° to represent ‘0’ and ‘1’. This protocol is much easier to implement but security proofs have not yet been developed to show that it is absolutely secure.

- Six state protocol uses three pairs of orthogonal polarisation states to represent the '0' and '1'. It is less efficient in transmitting keys but can cope with higher levels of error than BB84 or B92.

A different QC approach relies upon the EPR protocol invented by Professor Ekert of Cambridge University in 1991, which uses the property of 'entanglement'. EPR refers to Einstein, Podolsky and Rosen who first described the apparent paradox by which the quantum properties of two photons (such as polarisation) can be 'entangled' so that a measurement on one gives 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 with polarisation, and if one is transmitted and the other retained by the sender, then when the recipient makes a measurement both parties will automatically know the polarisation of each others' photon. An EPR source inherently produces photons with one of two orthogonal polarisations at random. For QC the EPR is set up to produce photons according to the BB84 protocol with four different polarisation states. It differs from BB84 in that the polarisation generation is inherently random. Once again any attempt at eavesdropping may be measured by its impact upon the photons received.

The BB84 protocol is easier to realise in practice than EPR and is used in most current implementations. This is because current EPR sources do not generate enough photons to compensate for optical losses and its range is therefore restricted.

The BB84 QC Protocol

BB84 was the first provably secure protocol for QC, named after its inventors Bennett and Brassard in 1984. Each bit of information is encoded as the polarisation state of a single photon of light. A practical QC protocol has to overcome two specific problems

- In real systems, not all of the photons transmitted will be received, due to natural losses in the transmission medium. Therefore, some means needs to be provided for the transmitter (traditionally called Alice) to confirm which photons reached the recipient (traditionally called Bob).

- An eavesdropper (traditionally called Eve) may know that information is encoded as one of two polarisation states. She could sit in the middle of the communications and make direct measurements on the photons because she has prior knowledge.

This protocol employs two stages

- Quantum Key Distribution (QKD). In this process an ambiguity is deliberately introduced by randomly changing between two different bases ($0^\circ/90^\circ$ or $-45^\circ/45^\circ$) to represent a '1' and a '0' (i.e. four different polarisation states in all). Measurement is achieved by using a polariser in the appropriate one of the two orientations. Because the correct orientation is changing at random, Eve can never be certain which one to use, and will introduce errors when she has her polariser in the wrong orientation. This error rate uniquely identifies her presence. Overall without prior knowledge an error rate of 25% results for Bob as well as a potential Eve.
- A sifting process is then used where Alice and Bob communicate over a normal telephone line to confirm when Bob used a polariser in the same basis (i.e. either $0^\circ/90^\circ$ or $-45^\circ/45^\circ$) as sent by Alice. Only these photon bit values are retained, the others are discarded. Note the actual polarisation orientation is not revealed and therefore Eve does not know the bit value. This information is too late to be of any value to Eve.

Information theory can then reduce the potential information obtained by Eve to any arbitrary level. Classical error correction algorithms measure the error rate and remove these errors from the key sharing process. A further stage of privacy amplification can be used to reduce the shared key size by sacrificing bits so that the information potentially gained by Eve is reduced. Security proofs have been developed to show that BB84 is absolutely secure provided that the error rate is below certain levels.