**QUANTUM CRYPTOGRAPHY**

**Quantum cryptography** is a method of [encryption](https://www.techtarget.com/searchsecurity/definition/encryption) that uses the naturally occurring **properties of quantum mechanics** to secure and transmit data in a way that cannot be hacked.

Cryptography is the process of encrypting and protecting data so that only the person who has the right secret key can decrypt it. Quantum cryptography is different from traditional cryptographic systems in that it **relies on physics, rather than mathematics**, as the key aspect of its security model.

Quantum cryptography **uses individual particles of light, or photons**, to transmit data over fiber optic wire. The photons represent [binary](https://www.techtarget.com/whatis/definition/binary) bits. The security of the system relies on quantum mechanics. These secure properties include the following:

* **particles can exist in more than one place or state at a time;**
* **a quantum property cannot be observed without changing or disturbing it; and**
* **Whole particles cannot be copied.**

These properties make it impossible to measure the quantum state of any system without disturbing that system.

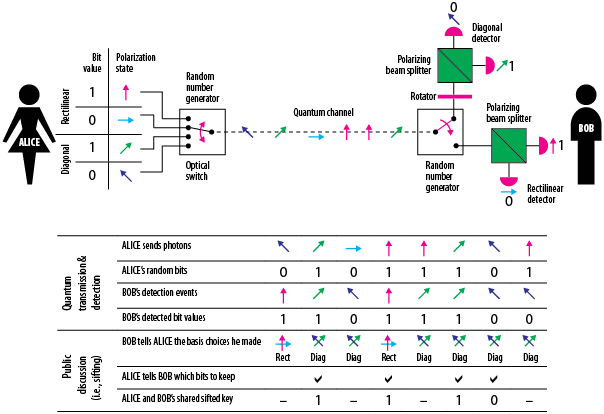
Photons are used for quantum cryptography because they offer all the necessary qualities needed: **Their behaviour is well understood, and they are information carriers in optical fibre cables**. One of the best-known examples of quantum cryptography currently is **quantum key distribution** ([QKD](https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD)), which provides a secure method for key exchange.

HOW QUANTUM CRYPTOGRAPHY WORKS

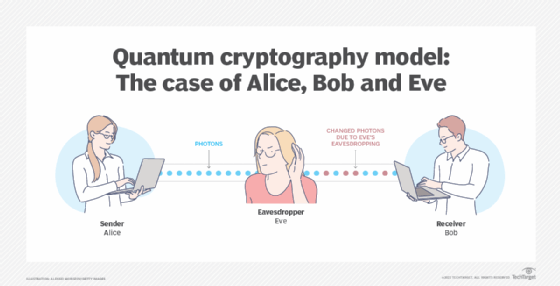
There are two people named **Alice and Bob** who wish to exchange a message securely. **Alice initiates the message by sending Bob a key**. **The key is a stream of photons** that travel in one direction. Each photon represents a single bit of data -- either a 0 or 1. However, in addition to their linear travel, these photons are oscillating, or vibrating, in a certain manner.

So, before Alice, the sender, initiates the message**, the photons travel through a polarizer.** The polarizer is a filter that enables certain photons to pass through it with the same vibrations and lets others pass through in a changed state of vibration. **The polarized states could be vertical (1 bit), horizontal (0 bit), 45 degrees right (1 bit) or 45 degrees left (0 bit).** The transmission has one of two polarizations representing a single bit, either 0 or 1, in either scheme she uses.

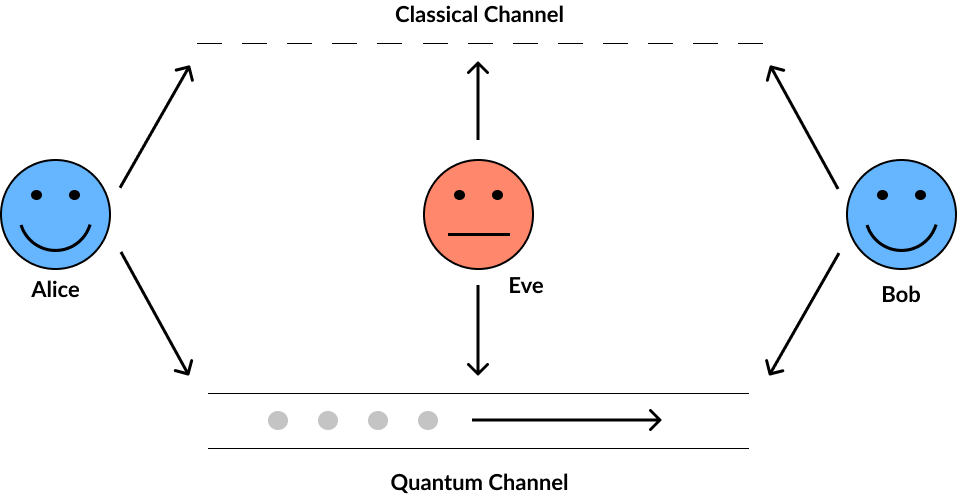
The photons now travel across optical fiber from the polarizer toward the receiver, Bob. This process **uses a beam splitter that reads the polarization of each photon.** When receiving the photon key, **Bob does not know the correct polarization of the photons, so one polarization is chosen at random.** **Alice now compares what Bob used to polarize** the key and then lets Bob know which polarizer she used to send each photon. Bob then confirms if he used the correct polarizer. **The photons read with the wrong splitter are then discarded, and the remaining sequence is considered the key.**



HOW QC PREVENTS EAVESDROPPING

Let's suppose there is an [eavesdropper](https://www.techtarget.com/searchunifiedcommunications/definition/eavesdropping) present, named Eve. Eve attempts to listen in and has the same tools as Bob. But **Bob has the advantage of speaking to Alice** to confirm which polarizer type was used for each photon; **Eve doesn't**. Eve ends up rendering the final key incorrectly.**Alice and Bob would also know if Eve was eavesdropping on them**. Eve observing the flow of photons would then change the photon positions that Alice and Bob expect to see.

**Quantum key distribution (QKD)**



## BB84 protocol

## The idea is to encode every bit of the secret key into the polarisation state of a single photon. Because the polarisation state of a single photon cannot be measured without destroying this photon, this information will be ‘fragile’ and not available to the eavesdropper. Any eavesdropper (called Eve) will have to detect the photon, and then she will either reveal herself or will have to re-send this photon. But then she will inevitably send a photon with a wrong polarisation state. This will lead to errors, and again the eavesdropper will reveal herself.

## B92 protocol

**B92 protocol is a modified version of the BB84 protocol** with the key difference between the two being that while BB84 protocol uses four different polarization states of photon, **the B92 protocol uses two (one from the rectilinear basis, conventionally H-polarization state and one from the diagonal basis, conventionally +45°-polarization state).**

## E91 protocol

## It is possible for two particles to become entangled such that when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible, however, to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observations over a classical channel. The process of communicating using entangled states, aided by a classical information channel, is known as quantum teleportation and is the basis of Ekert’s protocol