appeared on 21st Jan 2005

Lipstick on your collar

Quantum mechanics provides a way to mark messages that have been read before delivery, says S.Ananthananrayanan.

When we send a letter which is confidential, we often sign or draw two lines across the flap of the envelope. This is to help the receiver make out if the envelope had been opened en route.

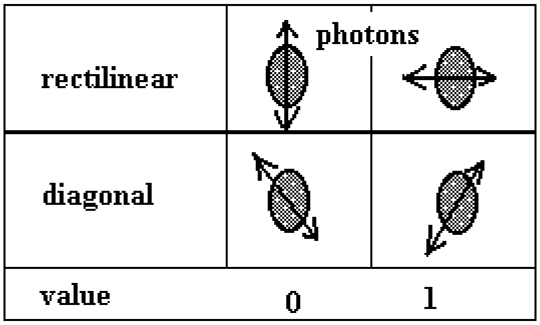
Computer communications

Much commerce is now being carried out over the Internet or other computer networks. To be sure that messages exchanged are genuine and also to make sure that the sender is not able to later deny having sent the message, commercial messages are often transmitted in code. A secret word or code number, which is the key to read the message, is known only to the sender and receiver. To make things even more secure, this code is changed frequently, often once for each message. But now it becomes crucial that the code be exchanged in complete secrecy.

Medium is message

If this code were sent by telephone, cable or wireless, there is no guarantee that nobody was listening in. What is worse, there is no way to know whether or not there had been an eavesdropper. But if the code word or number were conveyed through a stream of single photons, it turns out that any 'listening in' would leave a mark on the message itself.

The photon, or particle of light, has a property called polarization. This can be understood simply as 'orientation' – and we could fix it to be: up-down, right-left, diagonal to the left or diagonal to the right, like shown. And our code could be: up-down or diagonal to the left to mean '0' and left-right or diagonal to the right to mean '1'.



A series of photons could then encode a number consisting on '0's and '1's, the standard alphabet of computer communications.

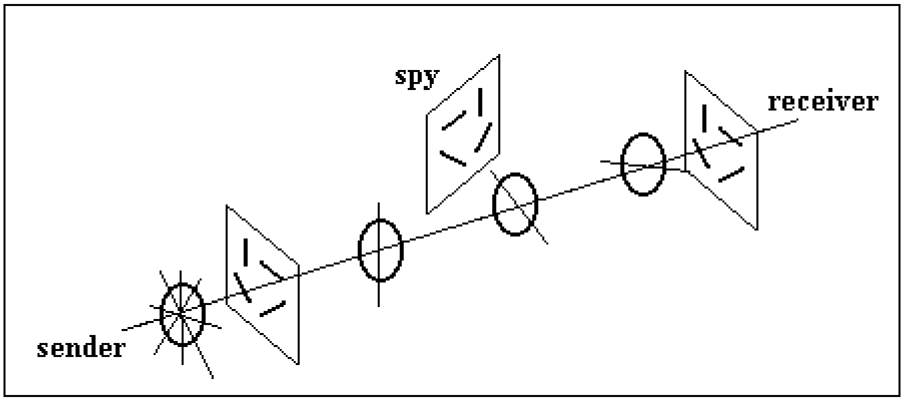
Enter quantum mechanics

The difference that QM makes is that the polarization state of a photon is not just one value but is in fact either or any of possible polarizations at the same time, with different likelihood of the two states to be found if there was a measurement. But once measured and found to be in some state, the photon is fixed in that state! This kind of 'statistical' property explains the behaviour of very small things, like inside atoms and molecules. But over large numbers of such small things, which is what ordinary objects like marbles, cricket balls or planets are, the rules add up to the good old Newton's laws.

Thus, a photon in the up-down state would pass correctly through an up-down filter and would not pass through a right-left filter. But with a diagonal filter, it would pass fifty percent of the time, and each time, it would end up as a diagonal photon, either left or right, depending on the filter used for detection. That is, rectilinear filters would detect rectilinear photons, but be uncertain of diagonal photons. And diagonal filters would detect diagonal photons but be uncertain of rectilinear photons.

Tainted messenger

A message consisting of photons in one of the four states is sent out. The receiver reads them with a random sequence of orientations of filters He will then end up with a message of '0's and '1's, but only the values where the filter had been correct would valid. After the message is over, he talks with the sender over the public telephone and tells her the sequence of filters he used. She tells him which filters had been correctly oriented, ie, rectilinear of diagonal. This would openly state which measurements were valid, but not disclose whether the measurements had been '0' or '1'. The value conveyed by the valid measurements would then form the secret code!



Intruder alert.

What if an eavesdropper had secretly measured the photons en route? Well, because of the way quantum mechanics works, every time he/she made a measurement with the wrong orientation of filter, the photons would have changed orientation. The values read by the receiver would no longer be what had been sent. The receiver and sender could verify a few of the valid signals and come to know if the message had been compromised!