11/16/2020 - Quantum Cryptography

Monday, November 16, 2020 11:32 AM

Summarizing Chapter 8 in The Code Book by Simon Singh

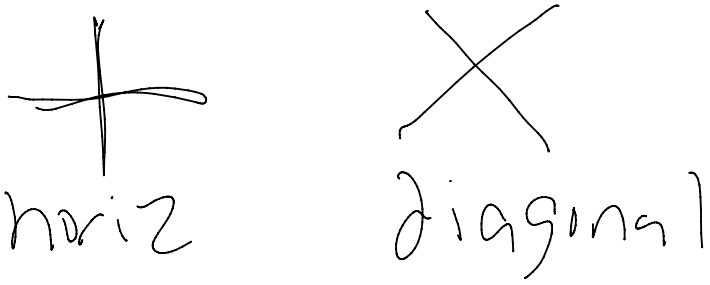
Can we make an unbreakable cipher?

We can send photons on a fiber optic cable. What's interesting about small particles is that on occasion, attempt to observe them changes them!!!

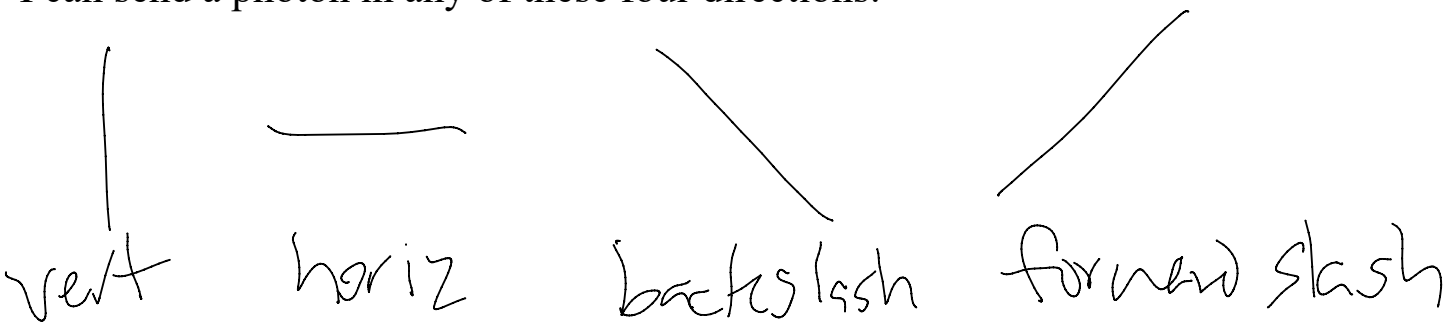
My example of this phenomenon: Whenever I tried to observe my daughter in pre-school to see what she was like without me there, invariably, she would recognize that I was there and this affected her behavior, so I could not really ever see, what she was like when I wasn't there…

Photons can be at different spins, but if you don't observe a photon, it can be in an "unknown" spin. But, if you try to observe it, you force the photon into a known spin. When you observe a photon you have to use a "reader" and that reader forces the photon into a particular type of state.

Readers:



I can send a photon in any of these four directions:



If I send a vertical or horizontal photon and try to read it with the

horizontal reader, 100% of the time, I will read the photon correctly as either horizontal or vertical.

If I send a backslash or forward slash and try to read it with the diagonal reader, 100% of the time, I will read the photon correctly as either a backslash or forward slash.

So if I just wanted to send some bits over a fiber optic cable, I could just ask the recipient to always use the horizontal reader and tell them that vertical was 0 and horizontal was 1…Or I could tell them to use a diagonal reader and set backslash to 0 and forward slash to 1.

If we did this, though, Eve could just set her reader somewhere (using the same reader as Alice) and read all the bits also…

If I send a vertical or horizontal photon, and try to read it with the diagonal reader, 50% of the time I'll read the correct bit and 50% of the time I'll read the wrong bit AND I will change the orientation of the photon to be either a backslash or forward slash.

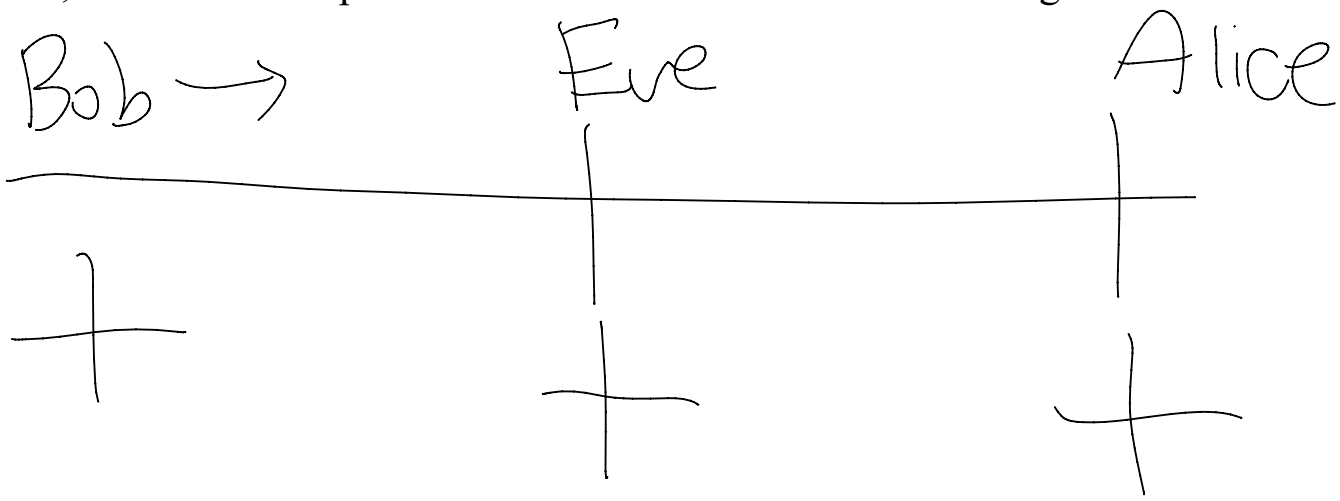
If I send a backslash or forward slash and try to read it with a horizontal reader, 50% of the time I'll read the correct bit, and 50% of the time I'll read the wrong bit AND I will change the orientation of the photon to be either horizontal or vertical.

Imagine we are Bob sending bits to Alice, but not using the same reader all the time, in fact, we randomly choose which reader to use. Also, imagine not telling Alice. In this set up with no one else listening, then Alice will use the correct reader about 50% of the time and the wrong reader 50% percent of the time.

So, if I am Bob and sending bits to Alice (say a secret shared key), I send 1000 bits in a random orientation. After I am done, I get on the phone with Alice and tell her which orientation I used for all the bits. She can cross check with her choice of readers and for about 500 bits, she will have used the correct reader, and the answer that she gets for those bits is what Bob had wanted to send.

So without saying on the phone WHAT the bits were, Alice and Bob can figure out which bits were properly sent over.

Take this picture, and imagine that Eve is eavesdropping. In order to do this, she has to set up a reader before Alice receive the message:



If this is my picture, Eve will always read the same thing as Alice.

In this picture, what Bob sends will definitely get turned into either a forward or backward slash and Eve will incorrect read what Bob meant 50% of the time, and then Alice will also read what Bob sent incorrectly 50% of the time, and about 50% of the time Eve and Alice will disagree.

The idea here is that, if Bob and Alice know they used the same reader, AND they decide to ask each other what bit was sent and received, AND those answers don't match, then they have proof that Eve was trying to listen!!! **No matter how "delicate" Eve is, she can NOT avoid being detected, because her reader can change the photon that is sent.**

Here is the idea, to exchange a secret key:

Bob sends Alice 1000 random bits.
They choose about 100 bits to sample.
For these 100 bits, they share which reader they used and which bit was sent and received. For 50 of these bits, roughly, the readers will match. If all 50 bits also match, then Alice and Bob will assume that no one was listening.

If someone had been listening, then the chance they used the wrong reader on those 50 bits is 50%, and then for the 25 bits that the wrong reader was used, the chance that Alice read all correctly is only $.5^{25}$, which is about 1 in 32 million. If you wanted to lower this probability, you would sample even more bits.

So in general, if we sample k bits, the probability that Eve can go undetected is $.5^{k/.4}$.

If any of these bits don't match, throw away the whole conversation…If they all match, then go back to remaining 900 bits, and share the orientation of all of them, so we would expect about 450 bits to remain where Bob and Alice used the same reader/orientation, and then these bits represent the secret key exchanged for which we are fairly certainly no one was listening.

You could either use these bits as a secret key for a private key scheme, or you could also use them as a one time pad…The latter would provide perfect security in theory, but also be very time consuming and expensive.

Drawbacks
Infrastructure isn't there for wide spread communication.
These lines are very, very expensive to build and don't span the globe.
They can go several miles though.
I am guessing that if any of this breaks, fixing the physical parts is quite difficult.

Advantages
In theory, could provide an extremely high, near perfect guarantee of secrecy.

The idea has been around for a long time (20+ years), but even in this time, it hasn't been used practically. Rather only in very small experiments.

To date, the longest distance over which a secret key has been transmitted is 421 kilometers.