Conservation of energy used to parallelize quantum key distribution

reader comments

0 with 0 posters participating

Share this story

It has been a while since I wrote about quantum key distribution. Once a technology is commercially available, my interest starts to fade. But commercial availability in this case hasn’t meant widespread use. Quantum key distribution has ended up a niche market because creating shared keys with it for more than one connection using a single device is so difficult.

That may all change now with a very inventive solution that makes use of all the best things: lasers, nonlinear optics, and conservation of energy.

Quantum key distribution in less than 500 words

The goal of quantum key distribution is to generate a random number that is securely shared between two people, always termed Alice and Bob. The shared random number is then used to seed classical encryption algorithms.

The rules of quantum mechanics are what allow Alice and Bob to securely generate a shared random number. The process looks

like the following: Alice generates a photon via two decisions made randomly. The first is the orientation of a measuring apparatus—vertical/horizontal or diagonal/anti-diagonal. The second is which axis the photon is polarized along—polarization is the spatial orientation of the electric field of the photon. That leaves the photon in one of four possible states, which we will call horizontal, vertical, diagonal, and anti-diagonal.

Bob does not know the settings that Alice has used and can only make a random choice for the orientation of his measurement apparatus: horizontal/vertical or diagonal/anti-diagonal. Bob ends up with a string of horizontal, vertical, diagonal, and anti-diagonal measurement results (one for each photon that Alice sends).

To understand how to make sense of these results, consider two cases: Alice sets her apparatus to horizontal/vertical and sends a vertically polarized photon. Bob sets his apparatus to horizontal/vertical and measures a vertically polarized photon. Everything is entirely predictable.

For the next photon, Alice sets her apparatus to horizontal/vertical and sends a horizontally polarized photon. But Bob has set his apparatus to diagonal/anti-diagonal. In this case, the photon sets off one of the detectors at random. Nothing is predictable.

To make sense of these results, Bob and Alice share the orientation settings of their apparatus but keep everything else secret. When they happen to have the same settings, Alice and Bob know that the measurements they made of the polarization of the photon will agree. All the other results are thrown out. The randomly generated polarization settings and measurements have generated a shared random number without the actual number being transmitted.

Conservation of energy spreads your secret

One of the key points of the distribution system above is that there are only two parties: Alice and Bob. Adding a third would mean that both Alice and Bob have to have a separate connection to the third party and generate another key. The equipment overhead makes that undesirable. This is where the latest bit of research comes in.

Before we get to the key generation and distribution part, let’s talk about the physical network that connects the parties together. Let’s imagine we have four parties: Alice, Bob, Chloe, and Dave, all of whom wish to have pair-wise encrypted communication. Each receiver is fed by a single optical fiber, but each fiber carries multiple signals using different wavelength channels. Thanks to this capacity, any two of the above group (say, Dave and Chloe) have a pair of channels that are unique to them.

The channels are filled in a very clever way. Alice has a device that generates pairs of photons. These photons are generated by splitting an incoming photon from a laser. The splitting process pairs up the photon’s polarizations (the technical term is entangled). We can then use conservation of energy to divide up the photon pairs among the channels.

Maybe an example is easiest. If the incoming laser has a wavelength of 775 nanometers, the photon split could produce a photon with a wavelength of 1,544.5 nanometers (in this system, that corresponds to channel 41), then the second photon must have a wavelength of 1,555.5 nanometers (which is channel 27). If Alice measures on channel 41 and Bob measures on channel 27, they are measuring a pair of photons that were created together. Given a clever assignment scheme, we can ensure that each pair of receivers in the network has a unique pair of channels and so is always measuring photons created

together.

The rest of the process relies on the same method described above to create a secure random number. Critically, by keeping track of the channels used, it’s possible to have a single apparatus handle creating random numbers for multiple pairs of devices.

Open secrets

No one else inside or outside the network knows that number. Indeed, if someone on the network were to measure the photons in either of those channels, doing so would disrupt the measurement process and reveal the eavesdropper’s presence (in practice, the eavesdropper is revealed by errors in the key generation process).

Splitting off the channels at the receiver end is not even necessary. Each receiver is connected via a length of fiber that is, in general, unique. So, the photon pairs have unique arrival times. By synchronizing the detectors, the different channels can be separated. This makes the receiver setup identical to that for a simple pair-wise quantum key distribution link.

In addition to being slow, the researchers’ system has a serious disadvantage. In commercial systems, we cheat. Instead of a true single-photon source, we use very weak laser light: a *mostly* single-photon source. This weakens the key generation process a little but reduces the cost a lot. In this system, it is absolutely critical that pairs of entangled photons are generated, meaning that each network requires a highly stabilized laser and a delicate nonlinear optical device. As much as I love me some delicate nonlinear optical devices, I am not sure anyone else does.

Nature, 2018, DOI: 10.1038/s41586-018-0766-y (About DOIs)

https://arstechnica.com/?p=1428937