Alt: One area in which… is cyber security, where the muscular prime factorisation prowess is predicted to make a merry mockery of our best existing secret-key methods. /

The emergence of Quantum Computing has thrown the world of cyber-security up in the air.

Start

At the heart of private communication measures is the establishment and distribution of encryption keys secretly and securely.

While the precocious/prodigious prime factorisation abilities of quantum computers seem set to make a mockery of our best existing cyber-security measures/cryprographic key methods, study of quantum communications has simultaneously unearthed a possible lifeline, in the form of a new secure key method, whose integrity against eavesdroppers comes with a cast iron guarantee, backed by the laws of quantum physics. At least in theory.

Meet Eve, the cardboard eavesdropper. She lurks in every theoretical communication model, able to instantly recognise any potential weakness, able to call on any and all existing resources to aid in its exploitation. A sleek and savage/ruthless operator/predator on a single-minded hunt for illicit data, intent on maximum personal damage to our two workaday communicators/cryptographers, Alice and Bob, (trying to set up a secret encryption key). Financially, socially, emotionally, Eve won't rest until maximum ruination is achieved.

Enter Quantum Key Distribution, a method

If A and B keep their base choices secure during the process, Eve cannot know them. If she wishes to simply intercept Alice's photon, and send another to Bob, and has found out the bases being used, the best she can do is pick randomly, as Bob would, and send her measured state on to Bob. On top of her 50% chance to guess the right basis, if she picks wrong, she still has a 50% chance to guess the right value, meaning she'll only be wrong a quarter of the time, however she'll never know which basis Alice used.

Afterwards, Alice and Bob share the sequence of bases they used over the phone. Eve has, of course, bugged the line and hears everything. Our courageous communicators discard all the results where they used different bases (roughly half), and sacrifice a section of the remaining code by confirming it over the insecure line. By analysing the compromised results, the error rate introduced by Eve’s unavoidable tampering, is increasingly easily identified, the more photons she greedily pilfers.

However, all is not lost for Eve, as it’s a long walk from chalkboard to lab, and she has far sneakier means at her disposal.

The real world introduces various problems such as environmental and atmospheric interference, inherent device inaccuracies, creeping alignment errors, and other physical limits to accuracy and scope.

Introducing relays every few km to expand a network scales badly (quote) at the mo...etc.

And sure enough, down amongst the decay, in with the interference, is Eve, trying to mask the sound of her snatching within the systemic noise.

Box 1

We can create, and transmit, photons with chosen qubit states encoded into their polarisation direction, so that if we align the emitter with the detector, a vertically polarised photon, or “up” corresponds to a 0 in our code, while horizontal polarisation, “right”, corresponds to a 1.

When a photon prepared as V, 0 reaches the door, it is measured as V, or 0, with certainty.

More interestingly, when we tilt either our emitter, or our door, relative to the other, rather than no photons entering the slot, the probabilities are shifted smoothly from one outcome towards the other, with our measurement still either V or H with overall certainty, but with a chance of each outcome. Unlike with mail, every photon is delivered, but half are then translated into the wrong language.

If we tilt our devices at 45 degrees to each other, a photon prepared in either state, V or H, will be measured as V or H with 50/50 chance, and the original

If we cut out the rotational polarisation, we don't want to get too crazy.

Stupid questions (link to interviews?)

So is the race now on for physicists in team QKD to scrabble rabidly ahead before physicist hacker teams blow banking wide open and steal the world's wealth? Do they ever have nightmares about Eve, and does it actually stand for "Evil"?

The answer to my questions is a flat no, yet many good questions remain to be answered. At UCL in London, Quantum Technology, Professor Sougato Bose takes more convincing, "What a load of...etc."

Box 1(old)

In the same way that we can decompose a 2D graph into x and y coordinated, so too can we decompose any spin representation into x, y, and z components. (fig). each of which can be either in the up or down state when measured.

A state that is prepared to be ‘up’ in one direction, z, for instance, would be measured as ‘up’ with 100% probability if we align our measurement device to the z-direction, but would be measured as ‘up’ or ‘down’ with equal probability, if we measure in either the ‘x’ or ‘y’ directions.

With any orientation we choose, we can name a z-direction, for instance, and prepare an ion, electron, or photon with spin is (prepared to be) aligned perfectly up or down in an arbitrary x-direction, will be poised exactly in between up and down if measured in the y- or x-directions.

In reality we also need to contend with interference from the environment - everything else in the world that interacts with our qubit (be it coded to the spin of an ion, or photon, or to any quantum-behaved property we can decompose in a suitable binary way.

Of course, everything else might also include malicious tampering by Eve, the customary cardboard eavesdropper, intent on nothing other that maximum personal damage to Alice and Bob, the rando schlubs sharing a secret code, physically, socially, emotionally, using any and all the data she can leech from the cracks in their quantum network.

Who knows? (as punchline of a QP joke)

Photons mean the same thing in any language that’s complex enough to hold the information, they just break down into different bricks (in a diff way)
