Beating cyber criminals with quantum solutions

March 18 2015, by Geoff Pryde

Binary systems are not enough if you want to improve security. Credit: Flickr/Ivan Plata, CC BY-NC-SA

As hackers get more sophisticated in their cyber crime efforts, we need to look to new technology to make our systems more secure, and potentially unhackable.

For some types of hacking, we already know the ultimate answer: quantum physics provides a way to share information with absolute security, guaranteed by the laws of nature.

The basic quantum communication idea is simple and elegant. But simple ideas often crash into real-world practicalities.

Fortunately, quantum physics research is providing even more sophisticated tools that will finish the job. The technology isn't mature yet, but it is coming.

The key to the problem

Here's the scenario: two parties, call them Alice and Bob, want to send secure messages over a network – perhaps credit card data for an online purchase.

Let's say they each have an identical list of random numbers that is private to them. They can use this list as a secret key to encode and send uncrackable messages. But how do they make the shared key in the first place?

With conventional methods that don't use quantum physics, Alice sends Bob a key that is made up of ordinary bits (0s and 1s) of information. But it is possible that the key may be intercepted, copied and then sent on without Alice or Bob's knowledge. This compromises security, because if the key is no longer private then others could use it to decrypt the the message that it encodes.

Clever mathematical techniques can make it difficult for Eve (an eavesdropping cyber criminal) to use an intercepted key. But with enough time, or with future quantum computers, the code can still be broken.

A secure quantum key

This is where quantum physics comes in. Let's start with the simple version. Alice sends Bob the key using quantum bits (qubits) instead of regular bits. To do this, she might use photons, which are individual particles of light.

Unlike regular computing bits, photon qubits can take on *both* 0 and 1 bit values at the same time. This is in the same way that Schrodinger's cat is both dead *and* alive in the famous thought experiment. The photon qubits can be prepared in ordinary 0 or 1 states, or in these strange superposition states, and choosing these randomly makes the key that Alice sends.

Photons obey Heisenberg's uncertainty principle so that if Eve measures them, she alters information they carry.

This alteration reveals the hack to Alice and Bob, who therefore throw away their key instead of using it to encode a message. If there is no hack, then they can use the private key to encode a message with absolute security.

This simple version of quantum key distribution (QKD) secures the channel – the optical fibre, for example – against intrusions.

But there are two other potential locations for hacking – Alice's photon-sending device, and Bob's photon-measuring device. The simple protocol assumes that these are both perfectly secure.

But how can Alice and Bob be sure that their device vendor is not in league with Eve? Cyber criminals are very good at setting up sophisticated networks, so how do you ever know whom to trust? What can solve this new problem, and similarly nasty variants?

What an (en)tangled web we weave

The answer is quantum entanglement. Two entangled photons have quantum-linked states: measuring the information stored in one photon tells us about the information in the other.

This effect holds even if the two photons are far apart, even if they are on opposite sides of the Earth.

It turns out that measuring the first photon always gives a random result, specifically, a random bit 0 or 1. Does that sound useful? It should -– if Alice and Bob each perform the same measurement on separate photons from an entangled pair, they will get a random, *but shared*, number. By repeating this on many entangled pairs they can generate a secret key.

Consider the following example. Alice makes an entangled pair of photons and sends one to Bob. If Alice's random measurement result has value 0, then Bob's measurement will yield a 0 as well.

On a second entangled pair, produced and distributed the same way, Alice may measure 1 and so Bob will measure 1 as well. Continuing, they build up a long string of shared random bits, which will form their secret key. Any attempt by Eve to measure one of the photons will break the entanglement, an effect that Alice and Bob can detect.

So if Alice and Bob can verify that they share entanglement, then the channel is proven trustworthy.

Not only that, but they can use their untrusted devices to check whether those very devices are really trustworthy.

Wait, what? That seems like asking a suspected con man whether or not he is lying. It can't work! But it *does* work. The information connection contained in entanglement is just too strong to be mimicked by hacked devices.

Quantum security in the real world

Researchers have developed several variations of entanglement-based techniques for secure communications with untrusted devices.

One recent experiment I conducted with my team used an entanglement-testing method called quantum steering. Steering gives up the security of Bob's device in exchange for robustness against real-world imperfections (information gets a bit mixed up in real, imperfect optical fibres).

But we recovered the security of Bob's measurement device by programming it with additional photon qubits. Because of Heisenberg's uncertainty principle, a hacked measurement device can't extract the information encoded in these extra programming photons, which is the knowledge required to cheat the steering test.

This is the weird world of quantum physics at its finest. Even though Bob's device is implementing the program's instructions, it can't learn everything about those instructions!

In essence, our steering approach should be simpler to implement than some of the alternative entanglement-based methods, and more robust to real-world imperfections than the others.

Coming soon

Where to from here? Commercial prototypes of simple QKD systems already exist, and have been used to protect channels in real-world tasks such as transferring information between bank branches.

But existing commercial devices have also been hacked by attacking Alice or Bob's devices, because they were designed to secure the channel alone. As we've seen, entanglement-based schemes for securing end devices have now been demonstrated. Hopefully these will reach a level of commercial maturity in the next five years or so.

To implement this kind of quantum communication security technology, users will require quantum links for sharing entanglement, as well as existing computer networks. A quantum link could be as simple as an optical fibre connecting two QKD devices, one for each of Alice and Bob, which in turn are plugged in to the communicating computers.

Longer or more complex links will likely require modifications of existing optical fibre networks with new quantum signal-boosting devices (call quantum repeaters) that are under development. But it's possible to also imagine mobile QKD-secured data transfer, such as using a quantum-enabled smart phone to interact with an ATM.

QKD technology will be applicable whenever transmitted information is the thing to be protected. Banking or financial details, personal data, email and health records are just a few examples of confidential information that it is desirable to securely send over an external data line.

But the technology doesn't directly apply to the task of protecting a computer against a direct hacking attack. It can't protect against hacks where someone guesses a password or employs a virus to obtain access to a user's account.

One might imagine that the same kind of quantum physics principles could be adapted to addressing those problems, and indeed this is an open research question.

So, while quantum communication won't solve all cyber crime it's good to know that, for some critical types of information transfer, hackers will be defeated by the very laws of nature. And that's a message you can share -– safely -– with your friends.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Beating cyber criminals with quantum solutions (2015, March 18) retrieved 27 April 2024 from https://phys.org/news/2015-03-cyber-criminals-quantum-solutions.html