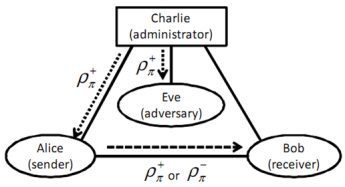

The fundamental problem of private communication is ensuring its security.

That's always been a tricky task but in recent years, cryptographers have added a powerful new weapon to their armoury: quantum key distribution. With this tool, it is possible to use the bizarre properties of the quantum world to send a message in such a way that guarantees its security.

The security of this system is a fact of nature. In the language of cryptography, quantum key distribution it is information-theoretically secure.

Although this sounds perfect, it does have some drawbacks. One of them is that while it is useful for one to one communication, it's not so good for universal communication over a network. That's because everybody on the network has to swap a secret key with everybody else to ensure they can chat securely. And that introduces a significant communications overhead.

In the 1970s, cryptographers came up with a way around this problem: so-called public key encryption. This is a form of encryption in which anybody can encrypt a message using a public key but only those with another private key can decrypt the message.

This kind of asymmetry is possible because of certain mathematical functions that are easy to perform in one direction but hard to do in reverse. The most famous example is multiplication. It's easy to multiply two numbers together to get a third but hard to start with the third number and work out its factors.

This type of encryption is not information-theoretically secure since it is always possible to work out the factors of any number. The security comes from making the number so big that it is impractical to factorise it in a reasonable time frame, such as the life time of the universe. This kind of encryption is called computationally secure.

The problem with public key encryption schemes is that although classical computers cannot factorise big numbers quickly, quantum computers can. So as soon as the first decent-sized quantum computer is switched on, these kinds of systems will become insecure.

Today, Akinori Kawachi at the Tokyo Institute of Technology in Japan and a few buddies suggest that all is not lost for public key encryption. These guys have discovered a quantum problem that is hard to solve in one direction but easy to do in reverse. And they say this asymmetry could form the basis of a new kind of quantum public key encryption system.

Their system is based on the problem of distinguishing between two ensembles of quantum states. This is similar to the problem of determining whether two graphs are identical, ie whether they correspond vertex-for-vertex and edge-for-edge.

A related problem, called the graph automorphism problem, is known to be hard even for a quantum computer and it is this that Kawachi and co base their system..

The thinking is that increasing the complexity of the graph can always make this problem practically impossible for a quantum computer to solve in a reasonable time.

However, if the structure of some subset of the graph is known, the problem can be solved

easily. So the trick is to keep this structure secret. This then serves as the private key for decoding messages, while the graph itself is made public for encoding the message.

Kawachi and co say the quantum ensemble version of this problem could be used as the basis of public key cryptography which is computationally secure, even against attack from a quantum computer.

But don't expect to see this any time soon. We'll need a quantum internet first. But also quantum cryptographers will need to convince themselves that it really is secure, that there isn't some overlooked mathematical trick that could suddenly make the problem tractable.

That could take years, perhaps decades.

In the meantime, it'll be a nail-biting wait for Kawachi and co.

Source: TechnologyReview.com