Every day, we share information about ourselves over telephone calls, email messages and internet transactions. Our lives are increasingly digitised and our social connections literally networked. Thanks to United States government documents leaked last year, we know how little of this data traffic is private.

Even encrypted data is vulnerable. In documents disclosed by Edward Snowden, the US National Security Agency was revealed to have a programme called Penetrating Hard Targets with a goal of cracking strong encryption. An element was “to determine if, and how, a cryptologically useful quantum computer can be built”.

It is well known that a quantum computer, which uses physics inaccessible to conventional computers to speed up calculations, can crack RSA — one of the most widely used encryption systems today.

This month, news of the Heartbleed bug in the implementation of supposedly secure Internet protocols reminds us that even well-meant attempts to protect us can go wrong.

So what can individuals, organisations and governments concerned about keeping our secrets do? What are the ultimate limits of privacy? Researchers in Singapore and elsewhere are developing a form of cryptography that could end the long-running battle between code-makers and code-breakers. It promises that we can communicate secretly even when we do not trust our devices; we can certify their security without knowing every detail of their implementation.

What’s more, the scheme is resistant to enemies with superior technology. It can be safeguarded by the most powerful adversaries you can possibly imagine and still keep your data secure.

**THE QUANTUM OF SOLACE**

When technical buzzwords are stripped away, all we need to communicate secretly is a sequence of random bits — just 1s and 0s. These bits make a cryptographic key.

To encrypt your message, you convert it into Is and Os, like the codes inside computers. Then, bit by bit, you add the key to your message. The random bits scramble the message. The result is easily deciphered by someone having the same cryptographic key, but cannot be cracked by anyone else.

For this technique to be secure, it is vital that the key bits are truly random, never reused and securely delivered. So, the problem is: How do we make and share such keys?

In 1991, I proposed a way to use quantum physics to distribute a cryptographic key. Unlike encryption techniques that get their security from being computationally hard to hack, quantum cryptography relies on the laws of physics for protection.

Quantum physics is our best description of how the world operates at its most fundamental level. It describes how individual particles of matter and light, atoms and photons, behave and interact. The scheme I invented shares a key between two people (let’s call them Alice and Bob) using pairs of quantum “entangled” photons.

A source of entangled photons can be placed anywhere — with Alice, Bob or adversarial Eve, on a satellite or in any location whatsoever — as long as Alice and Bob are able to receive photons from the source. These photons may be beamed through open air or, like light signals that carry Internet traffic, be sent through optical fibre.
Quantum physics may be key to keeping data safe

*CONTINUED FROM PAGE 12*

Alice and Bob measure the polarisation of each photon (polarisation is the phenomenon in which light points in a particular direction, like the polarised glare that sunglasses block) as being 1 or 0.

Quantum physics tells us the result for an individual photon is random, but that Alice and Bob's results for each pair must be correlated — they will match — thanks to their entanglement.

With a few extra steps, this is how Alice and Bob end up with matching cryptographic keys. Any eavesdropping attempt introduces a mismatch to the keys, which Alice and Bob can detect by openly comparing a portion and discarding the key if it is insecure.

Recently, my Singapore colleague Valerio Scarani and others showed this idea to be more powerful than I originally thought, pioneering the concept of “device-independent” cryptography. They realised you can certify the security of devices simply by checking the correlation of Alice and Bob's measurements.

As long as our devices pass the test, we can confidently use equipment bought from any source, including an adversary. Remarkably, this check even guarantees security if the enemy has technology that is beyond our knowledge. More recently still, we have discovered that we do not even need to completely trust ourselves.

Key distribution requires Alice and Bob to make random choices in the measurements they perform. What if these choices are manipulated; if we don’t have free will?

Thanks to the discovery of a quantum trick to perform “randomness amplification”, as long as our choices are not completely predictable, we can communicate secretly.

**MAKING IT REAL**

Quantum cryptography is not only an academic curiosity. Devices that perform simple quantum cryptography protocols are already in the market and have been used in banking and voting.

They do not do “device-independent cryptography” with entangled photons, but technology under development may sooner or later mature to the level at which such schemes can be implemented. This kind of cryptography is on the edge of being feasible in research labs.

Singapore is among the world leaders in this field. My colleagues at the Centre for Quantum Technologies here already demonstrated some years ago the cryptography scheme I had first proposed. Professor Christian Kurtsiefer and Assistant Professor Alexander Ling used lasers and telescopes on the rooftops of buildings to exchange a secret key across the NUS campus using entangled photons.

Now, we are working towards making the kind of correlation measurements that will certify device-independent schemes and developing compact, rugged quantum devices that can form nodes in a future quantum network.

We even plan to test a device on a satellite as satellites can distribute keys over long distances.

With world experts also in the theory of cryptography, everything is in place for us to make fast progress.

I think the day when we stop worrying about untrustworthy or incompetent providers of cryptographic services may not be that far away.