

# Table of Contents

Capturing the Photon Burp . . . . .	1
-------------------------------------	---



# Capturing the Photon Burp

By Peter Carty

The era of quantum technology is dawning. With quantum computing set to smash our existing ciphers, quantum encryption is providing a new set of uncrackable codes. But are the new codes completely secure? asks Peter Carty

The age of quantum technology is beginning. MagiQ Technologies in New York and ID Quantique in Geneva are marketing quantum cryptography equipment. So far it is expensive: MagiQ (pronounced 'magic') says that its products cost between \$50,000 and \$100,000, and that clients will include banks, insurers, government agencies and pharmaceutical businesses. And both companies' applications are restricted to 'point to point' – in which pairs of computers are linked with secure communication lines. But the technology is developing rapidly and another company, BBN Technologies of Cambridge, Massachusetts, is busy linking computers into the first quantum internet, or Q-NET.

All of the systems use lasers to fire light pulses down fibre optic cables. The polarisation patterns of the light particles – the spatial distributions of their waveforms – are the basis for the encoding. Attempts to intercept messages can be detected easily, because they fall foul of Heisenberg's uncertainty principle: measurement of sub-atomic particles alters their parameters.

Quantum technology has long been held up as the future of computing, but it is not surprising that its first application is in the field of encryption. The histories of computing and encoding technologies are intimately connected. The first modern computer, the Colossus machine, was developed in Britain during World War Two to crack the German enigma code.

Of course, uncrackable coding – uncrackable for the time being, that is – already exists. RSA protocols are based on the difficulties of factoring large prime numbers. A user-friendly RSA kit called PGP (Pretty Good Privacy) was devised by an American scientist called Phil Zimmerman and posted on the net way back in 1991. Advanced versions are freely available. PGP has frightened security agencies, which have lobbied for the right to retain keys for tapping purposes. They may find that they gain access to PGP just as quantum cryptography starts to spread more widely. This 'stable door' situation is nothing new: the history of cryptography is a long series of such leapfrogs by code makers and breakers.

Quantum computing, as opposed to quantum cryptography, is still some way off but its advent will render RSA protocols obsolete. This is because it will enable extremely rapid factoring of large primes to take place. Under the laws of quantum mechanics, sub-atomic particles can be thought of as occupying different states simultaneously. This property can be exploited to perform byte-level calculations simultaneously where conventional computers process them in sequence. Enormous advances in computing speed and power are in store.

In the meantime quantum cryptography might not be quite the breakthrough we have been waiting for. Expense is one drawback, though the costs of the equipment is likely to drop. Compatibility with the internet is likely to pose more of a problem. Most of the net is not based upon fibre optic cables, and attempts to use fibreless transmission have had limited success to date. And in spite of their vaunted impregnability, there are security gaps in existing quantum cryptography systems. Data is vulnerable at the point at which it is fed into the transmission apparatus. Once inside it might not be secure either, despite the theory. For example, a hacker could send tracer pulses down the lines and measure the polarisation of reflections. And the current generation of lasers 'burp' out excess photons which could be captured and measured by hackers. If human rights groups, criminals, terrorists and the rest of us want to stay ahead of the security agencies, we'll have to hope that the scientists and engineers can

sort out all of these snags.

Peter Carty <peter.carty AT tesco.net> is a writer and journalist