

MONITOR**Uncrackable beams of light**

Sep 4th 2003

From The Economist print edition

Quantum cryptography—hailed by theoreticians as the ultimate of uncrackable codes—is finally going commercial

IN THE 1992 film "Sneakers", the ostensible research topic of one of the main characters was something called "setec astronomy". This was an anagram of the words "too many secrets". The research was supposed to be about developing a method for decoding all existing encryption codes. Well, if that were ever the case, it certainly isn't any more—thanks to a start-up in Somerville, Massachusetts, called MagiQ.

MagiQ is in the final stages of testing a system for quantum cryptography, which it plans to release commercially within the next few months. Encryption engineers have long waxed lyrical about quantum cryptography, but this is among the very first commercial implementations. The advantage of quantum cryptography schemes is that the code they generate are simply not—even in theory—breakable.

The scheme devised by MagiQ, called Navajo, does not use quantum effects to transmit the secret data. Instead, it is the keys used to encrypt the data that rely on quantum theory. If these keys are changed frequently (up to 1,000 times a second in Navajo's case), the risk that an eavesdropper without the key would be able to decrypt the data can be proved mathematically to be zero. Of course, given the key, the task would become a trivial one.

Navajo transmits the changing key sequence over a secure fibre-optic link as a stream of polarised photons (indivisible particles of light). Because the polarisation reflects the amount of electromagnetic radiation allowed to radiate at an angle to a light beam's direction, it can be considered to be a measure of the angular dependence of the light.

Should an eavesdropper tap into the secure fibre-optic line, he would disrupt this stream of polarised photons by the very act of observing them—and the tampering could be instantly detected. By changing the key frequently, Navajo could turn an off-the-shelf encryption scheme such as AES (Advanced Encryption System) into something that was essentially uncrackable.

As in all good encryption schemes, Navajo employs an element of redundancy. The sender has two random-number generators. The first is used to generate a random stream of zeros and ones—part of which will form the key. The second random-number generator chooses which "polarisation basis" the sender will use to transmit a given bit of the key. The sender uses two different polarisation bases, which are at right-angles to one another. Only by measuring in the correct polarisation basis can a receiver see which bit was sent—otherwise the result is meaningless.

For each bit, the receiver arbitrarily chooses which polarisation basis to use. The sender and receiver then talk over an open channel and find out which bits they measured using the same

basis. These bits (about half of the total) then constitute the key. If someone has been eavesdropping, some of these bits will have been disrupted. In that case the receiver will be unable to decode the message, and will thus conclude that someone is listening in.

This much is standard quantum cryptography. What is harder is building the hardware that can do it quickly and cheaply enough to be commercially viable. MagiQ is in a race with a Swiss company called ID Quantique to be the first to do so, and currently appears to be in the lead.

Of course, if the quantum signal could be transmitted wirelessly, it would liberate users from the cost and constraints of a fibre-optic line. Bob Gelfond, MagiQ's founder and chief executive, is coy about the possibility. He admits that his firm is working on the idea, but is not saying anything at the moment.

For the time being, Navajo requires a dedicated fibre-optic link, which only large corporations or governments are likely to have. And it currently works only at distances of up to 50 kilometres. Any longer than that and random interference degrades the stream of photons and makes them unusable. But within these constraints, Navajo is fairly cheap. MagiQ plans to sell it for \$50,000 a set.

Given the glut of unused optical fibre buried beneath the streets of the world, MagiQ is optimistic about Navajo's prospects. Andrew Hammond, a vice-president at the company, reckons the market could potentially be worth more than \$1 billion a year, with much of the business coming from firms with valuable intellectual property, such as drugmakers and aircraft companies.