Flaws in the quantum cryptosystem

Technology

The only way for an Eavesdropper, conventionally named Eve, to find this key would be to measure Alice's bits in the connecting fibre optic cables directly. This is where the laws of quantum physics, where manufacturers have placed their guarantees, steps in. When Eve tries to measure the bits of the stream of photons, half the time the standard chosen by her would be incorrect. Her measurement of the state of the photon would destroy that state according to Heisenberg's Uncertainty Principle. Bob and Alice would therefore end up with incompatible keys. When Bob tries to use his key to decrypt Alice's encrypted message, it would produce nonsense, unlike a classical RSA crypto system. This is where the in built eavesdropper alarm system steps in, alerting the legitimate users to an intrusion.

Flaws in the Quantum Cryptosystem Of course this is how the system is meant to work ideally under completely hypothetical situations, when vastly simplified. It leaves the obvious questions: is too much faith being placed on the success of this project, and can security really be completely guaranteed?

It is not guaranteed that the key can always be established between Alice and Bob. There will always be noise created by imperfections in the communication links which have the ability to alter the photon states, causing the established keys to be slightly different from one another. Furthermore, the noise may be great enough to mask the activity of Eve from the legitimate users. If Alice and Bob do not have the ability to asses the level of noise above a certain security threat threshold, they would be vulnerable to intrusion without them even being aware of it.

This has led to several devious hacks being thought of by the very designers of quantum cryptography in an attempt to think one step ahead of Eve. One such hack thought up by a team at the University of Geneva is the 'Number Splitting Attack', whereby a weak spot is found in the connecting fibre optics where Eve can splice in a fibre optic cable of her own. This attack relies on the fact that lasers, including Alice's, can transmit two or three photons instead of just one.

When this occurs it is detected by Eve and the excess photons are diverted through her cable and stored. She then waits for the order of the standards, used to transmit and detect the stream of bits, to be revealed. The stored photons are then measured in the appropriate standard, revealing the encoded bits. The Number Splitting Attack would enable Eve to obtain part of the key established between Alice and Bob. Alternative protocols are being set up to attempt to change the way the users tell each other what measurement standards are being used.

Another clever hack called the 'Tracer Attack' again relies on a weak optic cable linking Alice and Bob being spliced with her own. Eve, using her own laser and photon detectors, sends tiny, seemingly insignificant, tracer pulses into the main optic cable towards Alice's laser where they are reflected back down to Eve's photon detectors. Alice's laser may be transmitting the 0 and 1 photons using two different lasers, or may be transmitting them from the same laser which reflects the 0's and 1's differently.

This attack therefore enables Eve to measure whether Alice transmitted a 0 or a 1 without even affecting her transmitted photons. Using the same

principle, Eve shines thousands of 'junk' photons towards Bob's detectors. Since detectors in practical applications do not have an infinite capability, Bob's over-worked detectors may leak copies of Alice's photons back into the fibre optic cables which are again collected by Eve.

Conclusion

Despite all the hype of absolute security, it is clear that we once again have to think before promising such ideals. The determined Eve will always be trying to keep up, and the imperfections of engineering, having difficulty producing precisions down to the photon level, will always provide opportunities for her to do so. Scientific teams will push the technology closer and closer to the ideal, but it is by no means a battle that will have an end.

There are some, however that may take a somewhat radical view, that perhaps the complete concealment of certain information is undesirable. Indeed the original architects of the internet intended to produce a system to enable the free exchange of information among people. One set of human beings devising what they believe to be the ultimate secure system has the potential of being bested by another set of human beings. The quest for absolute security may be considered equivalent to chasing a rainbow. This seems to be how it is and how it always would be. Perhaps it is how it