A quantum leap in codes for secure transmissions

Banks, intelligence agencies and governments may soon be using an uncrackable method of transporting their data.

According to Jennifer L Schenker, in an article written for the International Herald Tribune on 28/01/2004, scientists in Europe, Asia and the United States say they are close to producing a commercial product.

The scientists are talking about a technology called quantum cryptography, which secures data in a radically different way from today.

Until now, messages have been encrypted at one end and decrypted by the recipient. However, this means that information about the code has to be shared by at least two people via courier, or via a communications network, thus making the codes susceptible to interception.

Physics promises change by using tamper-proof photons.

Most of today's secure digital data communications are based on the use of very long prime numbers, called keys. Two keys are used: A private key, which only the sender has access to, and a public key, available to anyone. The two keys work together, so a message scrambled with a public key can be unscrambled only with the private key. Public key systems require that the sender know the recipient's public key to encrypt a message. So a global registry of public keys is required. However, given a powerful enough computer, it is possible to figure out the private key from the public key.

Quantum cryptography allows the secrecy of the key to be guaranteed and abolishes the need for trusting a registry. Single photons discrete particles of light are used to transfer the numeric keys. The photons are so delicate that if anyone or anything tries to spy on their travels through fiber optic cables, their encoded state will change. The sender and recipient immediately receive error messages making them aware of the interference and so know not to use the key.

Quantum cryptography is one of the first applications of quantum physics, which is expected to replace today's binary system of computing.

Scientists hope that, sometime between 2015 and 2020, binary bits will be encoded on particles like photons or electrons. These quantum bits would allow computers to perform multiple complex calculations simultaneously.

It is believed that quantum computing increases the processing power of computers so substantially that it will be a greater step than the move from the abacus to the calculating computer and quantum cryptography is the closest to near-term application. Hackers are expected to be able to eventually crack even the best security system in place today and the only thing that could stop them is quantum cryptography.

Quantum cryptography has already captured the interest of Visa International and MagiQ Technologies, a New York company, and id Quantique, based in Geneva, have both recently started selling quantum cryptography products. After years of research work, larger players like NEC, Toshiba and Hewlett-Packard also say they are getting closer to introducing products.

According to John Rarity, a professor at the University of Bristol in Britain, the cost of such a system could be several hundreds of thousands of dollars per company network. Rarity is

part of an $11 million, four-year European Union-financed project called Secure Communications with Quantum Computing that will start in March.

In June Toshiba Research Europe, which is working with Cambridge University on quantum cryptography research, set a record when it proved it could carry quantum encrypted messages up to 120 kilometers, or 75 miles, far enough for many applications in metropolitan areas, said Andrew Shields, head of the quantum information group at Toshiba's British research laboratory.

However, there is still a lot of work to do and plenty of kinks still have to be worked out. Quantum crypto messages sent over fiber optic cable cannot travel very far, and can only work point-to-point. In other words, it cannot travel over a network.

To successfully work in a networking environment and at greater distances quantum repeaters, a kind of rudimentary quantum computer, must be added to regenerate the quantum bits.

NEC claimed, in October, to have made progress on the components needed to make quantum repeaters, and Hewlett-Packard is also working on them. Tim Spiller, a senior scientist at Hewlett-Packard's European research laboratory in Bristol said he thinks they know how to potentially build those and they are possibly five years away.

Until then, banks or government agencies can start using the technology to communicate between nearby branch offices. You are going to see more point-to-point products this year, and soon after that there will be distributed systems that work in a campus environment. NEC is working in that area, said Simon Webster, manager of telecom consulting at NEC Europe.

Meanwhile, work on a different way of carrying quantum bits is also under way in both Europe and the United States. Researchers working separately in Britain, Austria and the U.S. national laboratories at Los Alamos, New Mexico, are experimenting with transmitting quantum keys through the air rather than over fiber optic lines. The idea is to send the quantum keys up to satellites and then down to another destination.

A global investment of about $50 million of public and private funds will be spent on quantum cryptography over the next three years, Rarity estimated.

This is such a fundamentally different way of thinking that engineers, systems analysts and people in every aspect of the security sector are going to have to rethink the way they do everything.

A great deal of work will have to be done that has nothing to do with the science, Ross said. Perfecting the technology in the lab is only the beginning.