GLOBEANDMAIL.COM

Data encryption about to make quantum leap

Researchers working at subatomic level promise security that's unbreachable

By GRANT BUCKLER

Thursday, September 22, 2005 Posted at 8:38 AM EDT

From Thursday's Globe and Mail

Even as recent computer security breaches underline the importance of protecting sensitive data, efforts to develop more powerful computers also threaten to render today's best encryption technologies useless.

Fortunately, a better data protection technique is being perfected to counter the faster computers and new tools that threaten to crack today's encryption techniques. And ironically, the threat and the possible answer are related.

Both rely on quantum theory, which deals with the behaviour of very small particles. While quantum-computing researchers are working to develop computers that will have enough power to easily crack the most secure encryption systems most organizations are using right now, quantum cryptography promises to usher in encryption that is unbreakable no matter how powerful the computer. And this new type of encryption technology is already beginning to appear in commercial data security products.

Two companies -- **ID Quantique SA** of Geneva and **MagIQ Technologies Inc.** of Somerville, Mass. -- have pioneered commercial quantum cryptography gear. The devices rely on the principle that, at the subatomic level, you cannot observe a particle without altering it in a detectable way. One such particle is the photon -- the most basic element of light.

This principle is being applied to cryptography. Encryption relies on a secret "key" -- usually a string of letters and numbers -- known to both parties. In quantum cryptography, this key is transmitted over optical fibre -- or potentially as a beam of light through the air -- with each bit in the key represented by one photon. An eavesdropper could still intercept this key, but anyone who does so cannot avoid altering its properties in the process. That means eavesdropping can be detected and compensated for by dropping bits that may have been intercepted, or by discarding the compromised key and starting over.

The actual data are transmitted normally after being encrypted using this specially transmitted key. Given enough encrypted data to work on, a powerful computer could still figure out the key, explains Grégoire Ribordy, founder and chief executive officer of ID Quantique, so the trick is to change keys constantly to ensure an eavesdropper never gets enough data to break the code. This isn't practical for today's encryption systems because the keys must be exchanged physically to ensure they're transferred securely; as a result, they are typically used for hours or even days. But quantum cryptography technology allows the key to change several times a second and be sent over the network, Mr. Ribordy says.

The downside to the technology is that today's quantum cryptography is limited to distances of 100 kilometres over fibre because encoding each bit in a single photon produces a weak signal. This is useful for transmitting data within a city or its surrounding area, says Barry Sanders, director of the Alberta Institute for Quantum Information Science at the University of Calgary, but not for transfers over longer distances.

There are several possible solutions to the distance problem, researchers say. One is to build quantum repeaters that amplify the signal at intervals. This is theoretically possible, Mr. Ribordy says, but none exists today. Another option, he says, is to create networks that relay data from point to point to point, with quantum keys for each link.

In a different approach, University of Toronto researchers led by Hoi-Kwong Lo, a professor of electrical and computer engineering and physics, recently claimed the first experimental implementation of a quantum decoy technique meant to boost the performance of quantum cryptography using decoy bits to help detect eavesdropping. This would permit a stronger signal that is capable of travelling farther without compromising security.

While researchers work to solve the distance limitations of quantum encryption, Martin Illsley, director of research at Accenture Technology Labs, a unit of consultancy Accenture Ltd., says government, the military and the financial industry are currently the primary markets for the shorter-range technology. He adds that securely backing up data is expected to be one of the fastest-growing commercial uses of quantum cryptography, since backup facilities are usually quite near the data centres they serve.

Robert Gelfond, founder and CEO of MagIQ Technologies, adds that quantum cryptography could prove valuable for "any large to mid-size enterprise with data to protect," and predicts it will see broader use in business within 18 to 24 months.

Eventually, he says, as costs come down and the equipment becomes more common, even small businesses and consumers might end up using a version of quantum encryption to protect their privacy on-line.