



>  
accenture

*High performance. Delivered.*

Point of View

By Roland Hengerer,  
Martin Illsley and  
David Black

## Quantum cryptography represents the next line of IT security

A breakthrough in quantum or molecular computing could leave today's computers—and IT security systems—in the dust. High performance organizations are already looking at how quantum cryptography can provide both competitive differentiation and a new line of defense against the cleverest marauders of the information age.

• Consulting • Technology • Outsourcing

Security is an endless game of cat and mouse. Throughout recorded history, people have built the castle walls higher and thicker, yet the cleverest marauders have eventually found a way inside. In today's world, billions in currency and intellectual property flow through the Internet, a now-indispensable channel for commerce but one that is continuously under siege from global hackers.

Beyond viruses and worms, Accenture Technology Labs believes that one of the biggest looming security threats to individual, company and government data is likely to come from breakthroughs in quantum or molecular computing—breakthroughs that will leave today's computers in the dust. Quantum computing, for example, promises an increase in processing power so dramatic it will be a "greater step than the move from the abacus to the calculating computer."<sup>1</sup>

This, in turn, will threaten the very foundation of data encryption today, which relies on long strings of numbers that are practically impossible to decipher with current computing resources. While quantum computing seems to be years from practical application, it could unleash a hacker's "killer app" that breaks through security defenses.

In response to this and other threats, pioneering businesses and government groups are looking to quantum cryptography, which also emerges from the field of quantum physics, to stay a step ahead of enterprising computer criminals. Researchers at Accenture believe that quantum cryptography offers an important new line of defense—as well as an opportunity for competitive differentiation for early adopters of the technology.

### "Key" strength of quantum cryptography

Any security system is only as strong as its weakest link. One weak link in today's data security systems is key distribution. Since recorded history, every code requires a "key" for decoding a secret message. Codes are encrypted at one end and the recipient of the encoded text needs to know the key to decode the message.

# Early adopters: banks, intelligence, telecom

Early beneficiaries of this technology will include industries ranging from biotechnology to telecommunications, as well as government sectors such as intelligence and the military.

Banks, brokerage firms and other financial services companies are likely to be among the early adopters because of the high potential for loss and the global regulatory demand for tighter financial controls. Bank Austria-Creditanstalt made history in 2004 with the first demonstration of a bank transfer aided by quantum key distribution. In addition, quantum cryptography has captured the interest of Visa International, the credit-card giant representing some 21,000 banks.<sup>2</sup>

The Defense Advanced Research Projects Agency (DARPA), the central research and development organization for the US Department of Defense, has shown a keen interest as well. The DARPA Quantum Network became operational in October 2003 and has run continuously since. This network employs quantum cryptography to provide unprecedented levels of security for Internet traffic flows such as Web-browsing, e-commerce and streaming video.

Some telecommunications companies may consider quantum cryptography as an extra security offering—a market differentiator vis-à-vis the competition, especially given growing consumer awareness and concern over data security.

Corporate and defense IT systems today are secure due to increasingly sophisticated and complex encryption technologies. Many corporate “road warriors” carry small electronic devices that generate a long, randomly selected number to gain access to a network. This key changes automatically, for example every 60 seconds. These systems are reasonably effective unless the devices that generate the numeric keys are lost, stolen, or the global registry of keys becomes compromised, deliberately or inadvertently.

Quantum cryptography addresses this weak link of classical cryptography by using single photons—discrete particles of light—transfer the numeric keys. The photons are such that if anyone or any device tries to spy on their movement, the state of the photons changes and indicates the presence of an intruder, rendering them tamper-proof.

Quantum key delivery provides dual advantages of more secure key management and less human intervention. Key exchange is possible

as often as several times a second without slowing data transmission. Current systems for key generation and management have high overhead costs, which quantum key distribution could reduce since key management would be automated. Quantum physics also offers the promise of true randomness for on-demand key generation, something today’s digital technologies cannot guarantee.

## The state of quantum cryptography today

Fortunately, the development of quantum cryptography is further along than quantum computing, which still remains largely theoretical. With quantum cryptography products already commercially available, it is reassuring to see the proverbial barn door being secured before the birth of the horse destined to kick it open.

Two small companies—id Quantique of Geneva and MagiQ Technologies of New York—are the acknowledged leaders in developing quantum

“With quantum cryptography products already commercially available, it is reassuring to see the proverbial barn door being secured before the birth of the horse destined to kick it open.”

cryptography solutions. The first worldwide quantum key distribution system, id Quantique's Wise Key, went live in 2003. The same year, MagiQ announced successful end-to-end quantum communication with its Navajo Security Gateway. Both systems combine quantum key distribution with the data-communications hardware necessary to use existing fiber-optic connections.

Initial quantum cryptography systems don't require a physicist or an engineer to administer them; they fit in standard racks, plug into existing networks and claim reliability around the clock. The early plug-and-play systems cost US \$50,000-\$100,000.<sup>3</sup>

Quantum cryptography has limitations, but these are likely to fade in time. For example, the photon keys can travel only between computers directly connected through fiber-optic lines (as opposed to

networked systems), and the photons degenerate over long distances. Some large technology companies are examining how to extend the distance with quantum repeaters. Research is also under way for transmitting photon keys through the air rather than fiber-optic lines. Sending keys to satellites and down to another destination could help secure a global quantum internet.

For many companies, quantum cryptography will remain a futuristic solution for some time. But for others, quantum cryptography is already being considered a viable solution. Quantum key distribution, combined with the one-time pad encryption that is used to authenticate communication partners today, promises an unconditionally secure communication system. Consequently, quantum cryptography is drawing the interest of high performance organizations as a way to improve IT security.

"For many companies, quantum cryptography will remain a futuristic solution for some time. But for others, quantum cryptography is already being considered a viable solution."

## About Accenture Technology Labs

Accenture Technology Labs, the dedicated technology research and development (R&D) organization within Accenture, has been turning technology innovation into business results for almost 20 years. The Labs create a vision of how technology will shape the future and invent the next wave of cutting-edge business solutions. Working closely with Accenture's global network of specialists, Accenture Technology Labs helps clients innovate to achieve high business performance. The Labs are located in Chicago, Illinois; Palo Alto, California; and Sophia Antipolis, France. For more information, please visit our website at [www.accenture.com/accenturetechlabs](http://www.accenture.com/accenturetechlabs).

## A question of when, not if

Security professionals working "in the trenches" continue to deal with basic issues such as raising security awareness with users and managing systems. Today's encryption systems offer a high degree of security, assuming users understand and follow the recommended guidelines. Consequently, quantum cryptography remains on the periphery of their radar screens.

The history of cryptography, however, is a succession of apparently unbreakable codes that have been cracked. Confidential data stored with key lengths considered sufficient today might be decrypted by future computers. Sensitive military secrets, as well as valuable commercial data and trade formulas, must be protected not only today but for decades. Quantum cryptography offers a short term opportunity for competitive differentiation and the promise of long-term security against the cleverest marauders of the information age.

## About Accenture's Security Practice

Accenture's Security Practice is focused on the critical issues of security, trust, privacy and compliance. Accenture works with its clients to design innovative, tested security solutions that become part of an organizations core business processes and infrastructure. From addressing particular needs to providing end-to-end solutions to offering managed services, Accenture help address the most difficult security challenges. For more information, please visit [www.accenture.com/security](http://www.accenture.com/security).

1. "A quantum leap in codes for secure transmissions," International Herald Tribune, 28 January 2004.

2. Ibid.

3. "Quantum codes debut in real world," BBC News Online, 9 March 2004.