A Multi-Photon Approach in Quantum Cryptography

from the University of Oklahoma

Move over money, a new currency is helping make the world go round. As increasing volumes of data become accessible, transferable and, therefore, actionable, information is the treasure companies want to amass. To protect this wealth, organizations use cryptography, or coded messages, to secure information from "technology robbers." This group of hackers and malware creators increasingly is becoming more sophisticated at breaking encrypted information, leaving everyone and everything, including national security and global commerce, at risk.

But the threat to information breach may be drastically reduced as a result of a technology breakthrough that combines quantum mechanics and cryptography. University of Oklahoma electrical and computer engineering professor Pramode Verma and his colleagues Professor Subhash Kak from Oklahoma State University and Professor Yuhua Chen from the University of Houston have, at the OU-Tulsa College of Engineering labs, demonstrated a novel technique for cryptography that offers the potential of unconditional security.

"Unfortunately, all commercial cryptography techniques used today are based on what is known as computational security," Verma said. "This means that as computing power increases, they are increasingly susceptible to brute force and other attacks based on mathematical principles that can recover information without knowing the key to decode the information." Cryptography techniques based on quantum mechanics are not susceptible to such attacks under any imaginable condition.

In 2006, Kak postulated a theory known as the three-stage protocol, which relies on the unpredictability of photons to ensure hackers can't locate or replicate the information used to transmit information. The first laboratory demonstration of Kak's concept took place at the College of Engineering labs at the OU-Tulsa Schusterman Center. This is an important step toward the widespread adoption of Kak's discovery and may lead to a future in which, Verma said, "Basically, no matter how long or how hard they try, technology robbers can no longer decrypt or hack transmitted information."

This breakthrough has widespread economic and global applications. Quantum cryptography has been used in rare instances, primarily Swiss banks, but is limited by its short transmission distance and slow speed. Verma and his research team's technology demonstration suggest the potential for breaking those barriers.

"As we continue to test this promising method of quantum cryptology, we can

demonstrate its value and accelerate the adoption in the business world," Verma said.

The widespread application of quantum cryptology could someday ensure that technology robbers won't be able to break into the information bank.

For more information visit www.ou.edu *[1].*

Source URL (retrieved on *09/20/2014 - 9:12pm*):
http://www.wirelessdesignmag.com/news/2012/10/multi-photon-approach-quantum-cryptography?qt-most_popular=0

Links:
[1] http://www.ou.edu