First quantum cryptographic data network demonstrated

August 28 2006

A joint collaboration between Northwestern University and BBN Technologies of Cambridge, Mass., has led to the first demonstration of a truly quantum cryptographic data network. By integrating quantum noise protected data encryption (quantum data encryption or QDE for short) with Quantum Key Distribution (QKD), the researchers have developed a complete data communication system with extraordinary resilience to eavesdropping.

"The volume and type of sensitive information being transmitted over data networks continues to grow at a remarkable pace," said Prem Kumar, professor of electrical engineering and computer science at Northwestern's Robert R. McCormick School of Engineering and Applied Science and co-principal investigator on the project. "New cryptographic methods are needed to continue ensuring that the privacy and safety of each user's information is secure."

Kumar's research team recently demonstrated a new way of encrypting data that relies on both traditional algorithms and on physical principles. This QDE method, called AlphaEta, makes use of the inherent and irreducible quantum noise in laser light to enhance the security of the system and makes eavesdropping much more difficult. Unlike most other physical encryption methods, AlphaEta maintains performance on par with traditional optical communications links and is compatible with standard fiber optical networks.

The Northwestern researchers have previously carried out several

demonstrations of the compatibility and reach of the AlphaEta system in conventional wave-division multiplexed optical networks. However, in all these tests the communicating parties, called Alice and Bob, had pre-shared encryption keys for use in the AlphaEta system.

Quantum Key Distribution exploits the unique properties of quantum mechanics to securely distribute electronic keys between two parties. Unlike traditional key distribution, the security of QKD can in theory provide quantitatively secure keys regardless of advances in technology. Typically, these ultra-secure keys would be used in traditional encryption algorithms to allow for high-speed encrypted communications.

BBN has built and demonstrated the world's first quantum network with untrusted network switches, delivering end-to-end key distribution via high-speed QKD since 2004. With the Boston Metro QKD network running 24/7, it is evident that quantum cryptography works in practice and may provide a technique for building highly secure networks.

In the present advance reported here, the QKD and the QDE technologies have been interfaced together. This integration of BBN's QKD system, which constantly provides refreshed ultra-secure encryption keys, with Northwestern's AlphaEta encryption system forms a truly quantum cryptographic data network.

The combined QKD/AlphaEta system has been demonstrated in a nine kilometer link between BBN headquarters and Harvard University in Cambridge, Mass. The AlphaEta encrypted signal carried OC-3 (155Mb/s) SONET data between the two nodes. A fresh encryption key of about 1 kilobit was repetitively loaded every three seconds. In a separate test, the AlphaEta encrypted signal was looped back multiple times to create an effective 36 kilometer link where more than 300 consecutive key exchanges were demonstrated.

"As secure communications require both secure key distribution and strong encryption mechanisms, the combined QKD/AlphaEta system represents the state-of-the-art in ultra-secure high-speed optical communications," said Henry Yeh, director of programs at BBN Technologies.

Source: Northwestern University