Forget Quantum Encryption, Simple Scheme Can Stop Electronic Eavesdroppers

December 9 2005

James Bond may use the fanciest, most expensive and high-tech devices to thwart would-be eavesdroppers, but in a pinch, the super-spy can use one Texas A&M engineer's simple, low-cost scheme to keep data secure from the bad guys.

Dr. Laszlo Kish, an associate professor in the Department of Electrical and Computer Engineering at Texas A&M, proposed that a simple pair of resistors on the ends of a communications wire such as a phone or

computer line could keep eavesdroppers from intercepting secret messages. Added electronic disturbances (called "noise") or the natural thermal noise (called Johnson noise) produced by the resistors makes the scheme function and keep the message secret.

Kish's paper, "Totally secure classical communication utilizing Johnson(-like) noise and Kirchoff's Law," in which he proposes his communications scheme, has been accepted for publication in an upcoming issue of the journal *Physics Letters A*. (A preprint of the paper is available online at www.arxiv.org/abs/physics/0509136) The paper was also featured in a recent issue of *Science* (vol. 309, p. 2148, 2005).

Kish said that quantum encryption -- communicating with single quantum particles, where one particle carries a single bit of information -- is considered absolutely secure because any eavesdropper will be discovered by the extra noise the eavesdropper introduces into the communication channel as soon as the eavesdropper tries to extract "noisy" information, or bits, from the channel. But Kish said quantum encryption is very fragile and is limited by expense, vibrations, thermal gradients, maintenance needs, speed and distance.

Instead, Kish has proposed a classical, not quantum, encryption scheme that relies on classical physical properties -- current and voltage. He said his scheme is absolutely secure, fast, robust, inexpensive and maintenance-free and relies on simultaneous encrypting of information by both the sender and the receiver.

Picture a line of communication -- the line connecting two telephones or computers. The sender and receiver at each end of the communication line each have two resistors of different resistance. Each randomly connects a resistor between their ends of the wire and ground, and then the sender begins transmitting the message. Using the natural thermal noise produced by the resistors provides stealth, making the

communication difficult to discover.

While the line of communication is open, both the sender and receiver monitor the electrical current and voltage in the line. If both the sender and receiver use the larger resistances, the fluctuations, or Johnson noise, in the voltage will be large, while the fluctuations will be small if both use the smaller resistances. If one uses the larger and the other uses the smaller resistance, the fluctuations will be somewhere in between.

Of course, an eavesdropper can also measure this noise, but this intermediate level produced by a pair of large and small resistors provides secure communications, Kish said. Because the sender and receiver use different resistances, the eavesdropper cannot determine the actual location of the resistors or whether it's the sender or the receiver using the large resistance.

The only way an eavesdropper can determine which resistance is being used at which end is to inject current into the communication channel and measure the voltage and current changes in different directions. Doing this, though, exposes the eavesdropper, who is discovered with the very first bit of information extracted. And when an eavesdropper is uncovered, the sender or receiver immediately terminates the transmission of the message before the spy can extract any more information.

"The way the eavesdropper gets discovered is that both the sender and the receiver are continuously measuring the current and comparing the data," Kish said. "If the current values are different at the two sides, that means that the eavesdropper has broken the code of a single bit. Thus the communication has to be terminated immediately."

Kish said that the dogma so far has been that only quantum communication can be absolutely secure and that about $1 billion is

spent annually on quantum communication research.

"But my paper proves that classical communication measuring voltage and current can also be secure if we are doing that wisely, and it can be done much more cheaply and more easily than quantum communication," Kish said. "And it's superior to quantum communication because the eavesdropper has to break a few thousands of bits to get discovered in quantum communication. In my scheme, the eavesdropper can extract only a single bit before getting discovered."

Kish directs the Fluctuation and Noise Exploitation Laboratory in the electrical and computer engineering department and is also a researcher in the Electrical and Computer Engineering Division of the Texas Engineering Experiment Station, the engineering research agency of the State of Texas and a member of The Texas A&M University System. TEES administers Kish's research.

Source: Texas A&M University (by Lesley Kriewald), Image: audiopromoter.de