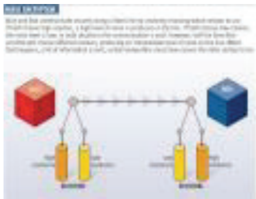
NewScientistTech

Home | News | Forums | Special Reports | Subscribe | Search | RSS

Noise keeps spooks out of the loop

23 May 2007
NewScientist.com news service
D. Jason Palmer

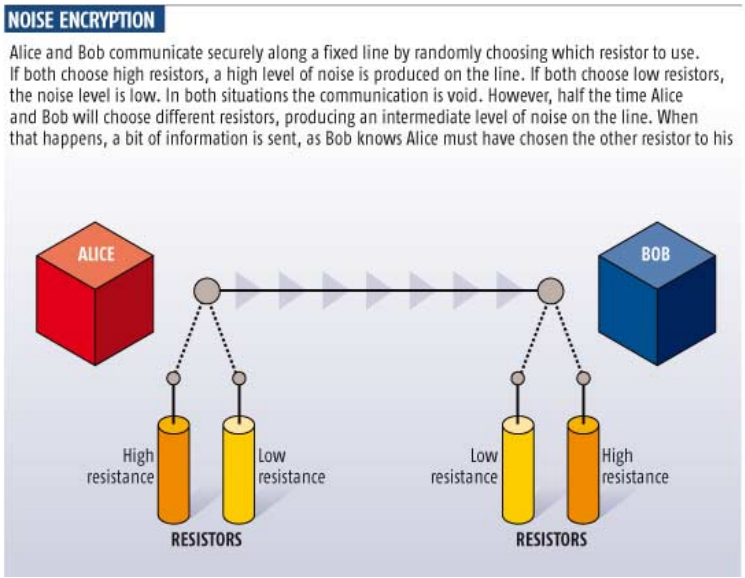


Enlarge image
Noise encryption

SPYING is big business, and avoiding being spied on an even bigger one. So imagine if someone came up with a simple, cheap way of encrypting messages that is almost impossible to hack into?

American computer engineer Laszlo Kish at Texas A&M University in College Station claims to have done just that. He says the thermal properties of a simple wire can be exploited to create a secure communications channel, one that outperforms quantum cryptography keys.

His cipher device, which he first proposed in 2005, exploits a property called thermal noise. Thermal noise is generated by the natural agitation of electrons within a conductor, which happens regardless of any voltage passed through it. But it does change depending on the conductor's resistance.



NOISE ENCRYPTION

Alice and Bob communicate securely along a fixed line by randomly choosing which resistor to use. If both choose high resistors, a high level of noise is produced on the line. If both choose low resistors, the noise level is low. In both situations the communication is void. However, half the time Alice and Bob will choose different resistors, producing an intermediate level of noise on the line. When that happens, a bit of information is sent, as Bob knows Alice must have chosen the other resistor to his

Kish and his collaborators at the University of Szeged in Hungary say this can be used to securely pass information, or an encryption key, down any wire, including a telephone line or network cable. In their device, both the sender Alice and the receiver Bob have an identical pair of resistors, one producing high resistance, the other low resistance. The higher the total resistance on the line, the greater the thermal noise.

Both Alice and Bob randomly choose which resistor to use. A quarter of the time they will both choose the high resistor, producing a lot of noise on the line, while a quarter of the time they will both choose the low resistor, producing little noise. If either detect a high or a low amount of noise in the line, they ignore any communication.

Half the time, however, they will choose differently, producing an intermediate level of thermal noise, and it is now that a message can be sent. If Bob turns on his high resistor, and records an intermediate level of noise, he instantly knows that Alice has chosen her low resistor, in essence sending a bit of information such as 1 or 0. Kish's cipher does this many times, sending a random series of 1s and 0s that can form the basis of an encryption key, the researchers say (http://www.arxiv.org/abs/physics/0612153).

That message is also secure. For a start, as Kish notes, it takes an "educated eavesdropper" to even realise information is being sent when there seems to be just low-level noise on the line. If they do try to eavesdrop, they can only tell a message is being sent, not what it is, because it's impossible to tell whether Alice has a high or low resistor turned on, and whether the bit of information is a 1 or a 0. What's more, eavesdropping on the line will naturally alter the level of thermal noise, so Alice and Bob will know that someone is listening in.

Kish and his team have now successfully built a device that can send a secure message down a wire

2000 kilometres long, much further than the best quantum key distribution (QKD) devices tried so far. Tests show a signal sent via Kish's device is received with 99.98 per cent accuracy, and that a maximum of just 0.19 per cent of the bits sent are vulnerable to eavesdropping. The error rate is down to the inherent resistance of the wire, and choosing a larger wire in future models should help reduce it further.

However, this level of security already beats QKD. What's more, the system works with fixed lines, rather than the optical fibres used to carry photons of light at the heart of quantum encryption devices. It is also more robust, as QKD devices are vulnerable to corruption by dust, heat and vibration. It is also much cheaper. "I guess it's around a hundred dollars, at most," Kish says.

"This is a system that should be taken seriously," says security specialist Bruce Schneier, who founded network security firm BT Counterpane. He says he was seduced by the simplicity of the idea when it was first proposed by Kish, and now wants to see independent tests of the working model. "I desperately want someone to analyse it," he says. "Assuming it works, it's way better than quantum."

From issue 2605 of New Scientist magazine, 23 May 2007, page 32

Close this window