CRYPTOGRAPHY

Simple Noise May Stymie Spies Without Quantum Weirdness

With the grand ambition of sending unbreakable coded messages, some physicists are using exotic tools—streams of individual photons and quantum mechanics—to shut out prying eyes. But a wire and a few resistors may convey a message as securely, says a physicist who has devised a simple and—he claims—uncrackable scheme. The idea shows that "classical" methods might compete with budding "quantum cryptography," others say. "I believe in beautiful and simple ideas, and this is one of them," says János Bergou, a theorist at Hunter College of the City University of New York.

Stealth technology. A simple wire and resistors may send data securely.

Take the hypothetical secret sharers, Alice and Bob: They transform a message into binary numbers and use a numerical "key"—a secret string of random 0's and 1's—to scramble and unscramble it. Quantum cryptography allows them to pass the key under the nose of an eavesdropper, Eve, because she cannot measure the condition of a particle without affecting it. So if Alice and Bob encode the key in individual photons, Eve cannot read it without revealing herself.

But Alice and Bob might do just as well by measuring the electrical noise on the ends of a wire, says Laszlo Kish of Texas A&M University in College Station. In Kish's scheme, Alice and Bob have two resistors each, one with a big resistance and one with a small resistance. Each randomly connects one resistor or the other between his or her end of the wire and ground and measures the voltage between the wire and ground.

On average, that voltage is zero. But electrons in the resistors jiggle about with thermal energy, so the voltage fluctuates, and the size of the fluctuations, or "Johnson noise," depends on the resistances Alice and Bob choose. If both use the large resistance, the fluctuations will be big. If both use the small resistance, they will be small. And if one uses large and the other uses small, the noise takes an intermediate value.

Eve can measure the fluctuations, too. But when the noise is at its intermediate level, she cannot tell whether Alice or Bob has chosen the large resistance unless she injects a current, which will reveal her presence, as Kish describes in a paper posted on the Web site www.arxiv.org and submitted to the journal *Physics Letters A*. So Alice and Bob can use the large-small pairs to generate the key.

Making the scheme work over long distances may not be easy, says Weston Tew, a physicist at the National Institute of Standards and Technology in Gaithersburg, Maryland. And Bergou notes that if the wire itself has a sizable resistance, then the fluctuations should be slightly larger on the end with the large resistance, a fact Eve might exploit if she spies on both ends at once. Still, today's quantum technologies only approximate the uncrackable ideals, and Kish's idea suggests that simpler schemes might match their performance, says Julio Gea-Banacloche, a theorist at the University of Arkansas in Fayetteville. "The more I think about it," he says, "the more I think that within limits it's workable."

–ADRIAN CHO

CREDITS (TOP TO BOTTOM): M. MASSIMINI *ET AL.*, *SCIENCE*; PHOTODISC BLUE/GETTY IMAGES

Published by AAAS