More Secure Optical Communications Via 'Antisqueezed' Light

October 10 2006

Using light to transmit information – optical communication – is the basis of several technologies, most commonly fiber-optic cables, which are used in imaging and telecommunications. But sending information securely using light requires minimizing and compensating for loss as the light propagates between transmitter and receiver. And in the area of security, there is always room for improvement.

Enter researchers Tatsuya Tomaru and Masashi Ban from the Hitachi Advanced Research Laboratory in Japan. Recently, they figured out that more secure optical communications can be achieved using "antisqueezed" light. Their work is described in the September 13, 2006, online edition of *Physical Review A*.

"Antisqueezed light is tolerant of loss and amplification," Tomaru told *PhysOrg.com*. "It is well suited to optical communication."

Antisqueezing, rather nonintuitively, is one side effect of a process called squeezing, which (also nonintuitively) is not the mechanical action its name implies. Rather, understanding squeezing and antisqueezing begins by understanding the quantum nature of light – that light is inherently grainy, made up of basic units, or "quanta," called photons. And photons, like other particles, like to retain some mystery. A photon will allow either its position or its momentum to be measured with high precision – but not both. This limitation is known as the Heisenberg Uncertainty Principle.

That said, squeezed light – and by extension antisqueezed light – is defined by fluctuations in the precision of the photons' measured position and momentum. When the fluctuation (i.e. the error) of the measured momentum is “squeezed,” the fluctuation of the measured position must, in accordance with the Heisenberg Uncertainty Principle, become inflated, or “antisqueezed.”

So how can this make optical communications more secure? Mathematically speaking, when squeezed light is transmitted, the larger fluctuation – the antisqueezed component – dominates, and the squeezed component regresses to the natural fluctuations light experiences in a vacuum. But the antisqueezed component resists that pull; it is always beyond the vacuum fluctuation, even after loss and amplification. The result is a signal that is far more loss-tolerant. As a result, there are far fewer lost pieces for eavesdroppers to collect.

Tomaru and Ban assume real light signals that are encrypted prior to transmission, with the intended receiver equipped with the proper key to correctly un-encrypt the signal. An eavesdropping receiver would not know this key, and would be unlikely to correctly guess it. This is a common way to secure a transmission. Using antisqueezed light adds an extra measure of security.

“Antisqueezing is essential to differentiating between legitimate receivers and eavesdroppers,” said Tomaru. “Eavesdropping would be very difficult under these conditions.”

Citation: T. Tomaru and M. Ban, “Secure optical communication using antisqueezing.” *Phys. Rev. A* 74, 032312 (2006)