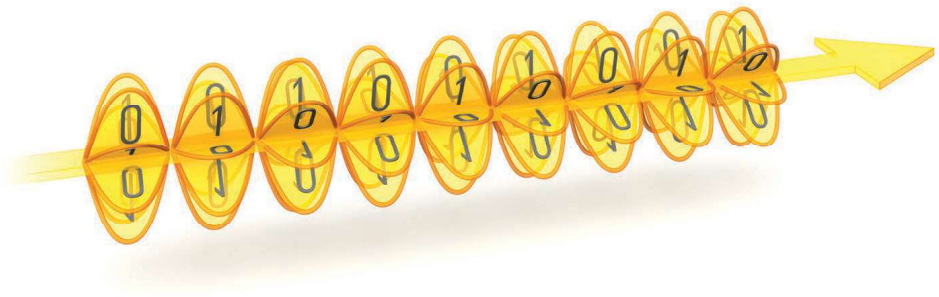

# NEW ENCRYPTION STRATEGY PASSES EARLY TEST

## Ghost polarization harnesses ultrafast fluctuations that occur in a light wave

**Telecommunications can** never be too secure. That's why researchers continue to explore new encryption methods. One emerging method is called ghost polarization communication, or GPC. Researchers at the Technical University of Darmstadt, in Germany, recently demonstrated this approach in a proof-of-principle experiment.

GPC uses unpolarized light to keep messages safe. Sunlight is unpolarized light, as are fluorescent and incandescent lights and LEDs. All light waves are made up of an electric field and a magnetic field propagating in the same direction through space. In unpolarized light, the orientation of the electric-field component of a light wave fluctuates randomly. That's the opposite of polarized light sources such as lasers, in which this orientation is fixed.

It's often easiest to imagine unpolarized light as having no specific orientation at all, since it changes on the order of nanoseconds. However, according to Wolfgang Elsaesser, one of the Darmstadt researchers who developed GPC, there's another way to look at it: "Unpolarized light can be viewed as a very fast distribution on the Poincaré sphere." (The Poincaré sphere is a common mathematical tool for visualizing polarized light.)

In other words, unpolarized light could be a source of rapidly generated random numbers that can be used to encode a message—if the changing polarization can be measured quickly enough and decoded at the receiver.

Suppose Alice wants to send Bob a message using GPC. Using the proof of principle that the Darmstadt team developed, Alice would pass unpolarized light through a half-wave plate to encode her message. A half-wave plate is a device that alters the polarization of a beam of light. In this specific case, the half-wave plate would alter the polarization according to the specific message being encoded.

Bob can decode the message only when he receives Alice's altered beam as well as a reference beam, and then correlates the two. Anyone attempting to listen in on the conversation by intercepting the altered beam would be stymied, because they'd have no reference against which to decode the message.

GPC earned its name because a message may be decoded only by using both the altered beam and a reference beam. "Ghost" refers to the entangled nature of the beams—separately, each one is useless. Only together can they transmit a message. And messages are sent via the beams' polarizations, hence "ghost polarization."

Elsaesser says GPC is possible with both wired and wireless communications setups. For the proof-of-principle tests, they relied largely on wired setups, which were slightly easier to measure than over-the-air tests. The group used standard commercial equipment, including fiber-optic cable and 1,550-nanometer light sources (1,550 nanometers is the most common wavelength of light used for fiber communications).

The Darmstadt group confirmed GPC was possible by encoding a short message by mapping 0 bits and 1 bits using polarization angles agreed upon by the sender and receiver. The receiver could decode the message by comparing the polarization angles of the reference beam with those of the altered beam containing the message. They also confirmed the message could not be decoded by an outside observer who did not have access to the reference beam.

However, Elsaesser stresses that the tests were preliminary. "The weakness at the moment," he says, "is that we have not concentrated on the modulation speed or the transmission speed." What mattered was proving that the idea could work. Elsaesser says this approach is similar to that taken for other forms of encryption, like chaos communications, that started out with low transmission speeds but have seen rates tick up as the techniques are refined.

Robert Boyd, a professor of optics at the University of Rochester, in N.Y., says that the most important question to answer about GPC is how it compares to the Rivest-Shamir-Adleman (RSA) system commonly used to encode messages today. Boyd suspects that the Darmstadt approach, like the RSA system, is not, in concept, absolutely secure. He says that if GPC turned out to be more secure or more efficient to implement even by a factor of two, it would have a tremendous advantage over the RSA.

Moving forward, Elsaesser already has ideas on how to simplify the Darmstadt system. And because the team has now demonstrated GPC with commercial components, Elsaesser expects that a refined GPC system could simply be plugged into existing networks for an easy security upgrade. —MICHAEL KOZIOL

**POST YOUR COMMENTS AT**
spectrum.ieee.org/cryptolight-jul2020

ILLUSTRATION BY Emily Cooper