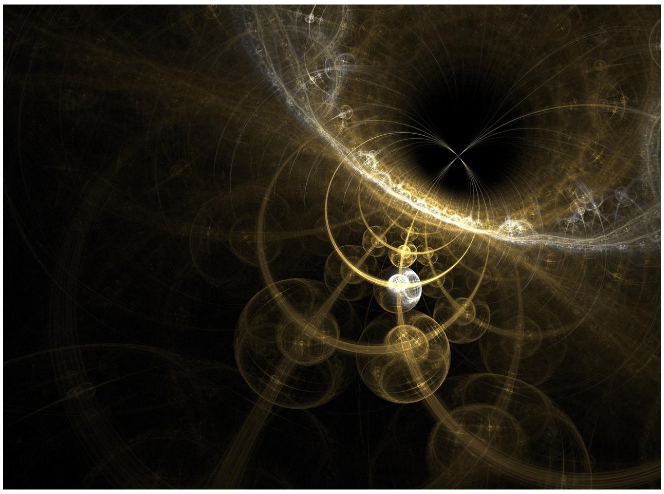
New all-fiber device simplifies free-space based quantum key distribution

6 May 2019



Credit: CC0 Public Domain

Researchers have developed a simple and stable device to generate the quantum states necessary for quantum key distribution. The device could make it more practical to develop a global data network that uses this very secure method of encryption to protect everything from credit card transactions to texts.

New encryption techniques are needed because computers powerful enough to crack today's algorithm-based encryption codes will likely be available in the next decade or two. Rather than relying on math, quantum key distribution uses quantum properties of light such as polarization to encode and send a random key needed to decrypt encoded data. The method is exceptionally secure because any third-party intrusion is detectable.

In the Optical Society (OSA) journal *Optics Letters*, researchers from the University of Padova in Italy report that their all-fiber device can switch the polarization of light more than 1 billion times per second. The device is also self-compensating, making it insensitive to temperature and other environmental changes.

"Quantum key distribution is expected to have a deep impact in the privacy and security of citizens," said Giuseppe Vallone, who led this research within the QuantumFuture research group coordinated by co-author Paolo Villoresi. "Our scheme simplifies quantum key distribution for free-space communication—such as from satellites to Earth or between moving terminals— which is required to achieve a global quantum network."

Developing a global network

Because quantum encryption doesn't work well over long-distance fiber networks there is now a push to develop a satellite-based quantum communication network to link various ground-based quantum encryption networks around the world.

Although various properties of light can be used to create quantum states for quantum encryption, polarization is particularly well suited for free-space links because it is not perturbed by the atmosphere and the decoding at the receiver can be performed without the challenging task of funneling the data into single mode fiber.

"Our goal is to develop a quantum encryption scheme to use between a satellite and the ground, where the keys are generated in orbit," said Vallone. "However, today's polarization encoders aren't ideal for use in space because they are unstable, expensive and complex. They can even exhibit side-channels that undermine the security of the protocol."

Fast and stable polarization encoding

The new polarization encoder—which the researchers call POGNAC for POlarization SaGNAC—can rapidly rotate the polarization of incoming laser light thanks to a fiber-loop Sagnac interferometer. This setup splits the light into two beams whose polarizations are at right angles relative to each other. The beams then travel through the fiber-loop in clockwise and counterclockwise directions. The current components could fit into a package measuring 15 X 5 x 5 centimeters, with further miniaturization possible if smaller components were incorporated.

Inside the fiber loop, the researchers used a commercially available electro-optics modulator to change the polarization to create the quantum states necessary for quantum key distribution. Because the clockwise and anticlockwise components arrive to the modulator at different times, they can each be modulated independently.

Modulators use an applied voltage to change the optical phase. However, the absolute value of the phase shift depends on many parameters that change with time. "In the POGNAC, only the relative shift between the two polarization components is relevant—this relative phase shift corresponds to a change in output polarization—while shifts that arise from temperature changes and other factors are self-corrected," said Vallone. "This makes the POGNAC very stable and eliminates polarization drifts that have affected other devices."

The researchers tested their new device by measuring the polarization of quantum states generated by the POGNAC and comparing them with the expected values. They measured an intrinsic quantum bit error rate (QBER) as low as 0.2 %, well below the 1-2 percent QBER of typical quantum key distribution systems.

"Our results show that data can be encoded using the polarization of light in a simple and efficient way," said Vallone. "We were able to accomplish this using only commercially available components."

The researchers are continuing to improve on their approach and plan to perform further tests to see how the POGNAC performs when encoding quantum keys for encryption.

More information: Costantino Agnesi et al, All-fiber self-compensating polarization encoder for quantum key distribution, *Optics Letters* (2019). DOI: 10.1364/OL.44.002398

Provided by The Optical Society

APA citation: New all-fiber device simplifies free-space based quantum key distribution (2019, May 6) retrieved 23 November 2020 from https://phys.org/news/2019-05-all-fiber-device-free-space-based-quantum.html