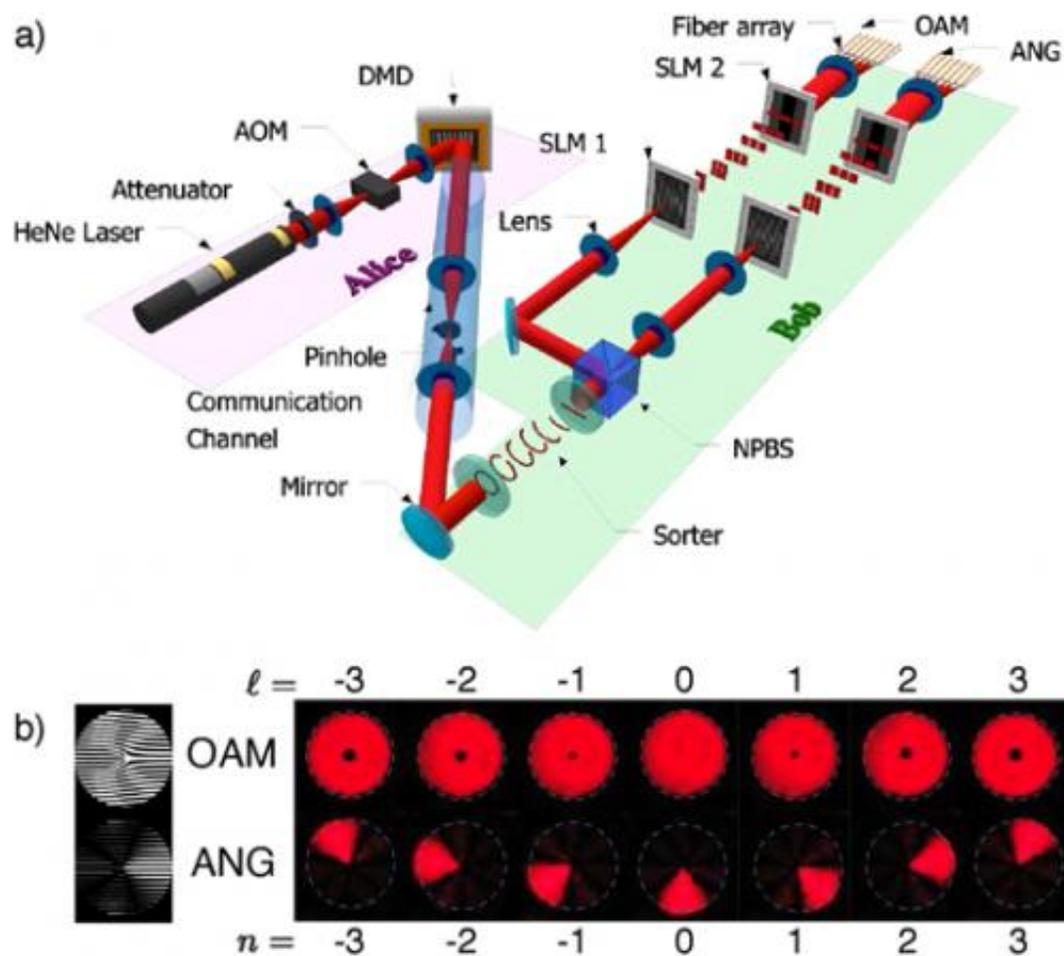


New approach uses 'twisted light' to increase efficiency of quantum cryptography systems

March 20 2015



(a) The experimental setup. Alice prepares the modes by carving out pulses from a highly attenuated He-Ne laser using an AOM. The spatial mode information is impressed on these pulses with a DMD. Bob's mode sorter and fan-out elements map the OAM modes and the ANG modes into separated spots that are collected by an array of fibers. (b) The alphabet. CCD images of produced light field profiles in two complementary spatial bases of OAM and ANG ($d =$

7). The intensity profile of the modes are shown on the right. An example of binary holograms used for the generation of modes in each basis is shown on the left. Credit: Mohammad Mirhosseini et al 2015 *New J. Phys.* 17 033033, doi:10.1088/1367-2630/17/3/033033

Researchers at the University of Rochester and their collaborators have developed a way to transfer 2.05 bits per photon by using "twisted light." This remarkable achievement is possible because the researchers used the orbital angular momentum of the photons to encode information, rather than the more commonly used polarization of light. The new approach doubles the 1 bit per photon that is possible with current systems that rely on light polarization and could help increase the efficiency of quantum cryptography systems.

Quantum cryptography promises more secure communications. The first step in such systems is [quantum key distribution](#) (QKD), to ensure that both the sender and receiver - usually referred to as Alice and Bob - are communicating in such a way that only they know what is being sent. They are the only ones who hold the "key" to the messages, and the systems are set up in such a way that the presence of any eavesdropper would be identified.

In the paper, published in *New Journal of Physics* today, Mohammad Mirhosseini and his colleagues describe a proof-of-principle experiment that shows that using OAM to encode information rather than polarization opens up the possibility of high-dimensional QKD. Mirhosseini, a Ph.D. student in Robert W. Boyd's group at the University of Rochester's Institute of Optics, explains that they were able to encode a seven dimensional "alphabet" - that is, seven letters or symbols - using both the [orbital angular momentum](#) (OAM) of the photons and their angular position (ANG). These two properties of the photons form what

physicists refer to as mutually unbiased bases, a requirement for QKD. Using mutually unbiased bases, the correct answer is revealed only if Alice encodes the information using a particular basis and Bob measures in that same basis.

In QKD, once they have generated a long, shared key, Alice and Bob publicly announce the basis (or "alphabet") they have used for each symbol in the key. They then compare what alphabet was used for sending and which one for receiving. They only keep the part of the key in which they have used the same "alphabet." The letters they keep produce a secure key, which they can use to encrypt messages and transmit these with regular encryption without the need for [quantum cryptography](#).

If for any reason their communication is intercepted, because of a fundamental property of quantum mechanics, there will be discrepancies between Alice and Bob's keys. To check for this, Alice and Bob sacrifice a short part of their key. They share this publicly and identify any discrepancies. This lets them know whether their connection is secure and, if not, they will stop the communication.

The researchers showed that using their system they were able to generate and detect information at a rate of 4kHz and with 93% accuracy. A long term goal of the research is to realize secure communications at GHz transmission rates, which is desirable for telecommunication applications.

"Our experiment shows that it is possible to use "twisted light" for QKD and that it doubles the capacity compared to using polarization," said Mirhosseini. "Unlike with polarization, where it is impossible to encode more than one bit per photon, "[twisted light](#)" could make it possible to encode several bits, and every extra bit of information encoded in a photon means fewer photons to generate and measure."

In a previous experiment using a strong laser beam instead of single photons, Boyd's team were able to measure up to 25 modes of OAM and ANG. This is equivalent to having 25 letters available in your "alphabet" rather than 7. This shows the potential for a system like the one described in the new paper to have the capacity to transmit and measure 4.17 bits per photon using more sophisticated equipment.

Mirhosseini acknowledges that the real-world challenges are not straightforward to overcome but when it comes to QKD, he is excited about the possibilities their system opens up.

More information: High-dimensional quantum cryptography with twisted light, Mohammad Mirhosseini et al 2015 *New J. Phys.* 17 033033, [DOI: 10.1088/1367-2630/17/3/033033](https://doi.org/10.1088/1367-2630/17/3/033033)

Provided by University of Rochester

Citation: New approach uses 'twisted light' to increase efficiency of quantum cryptography systems (2015, March 20) retrieved 26 April 2024 from <https://phys.org/news/2015-03-approach-efficiency-quantum-cryptography.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.