

Certifying Quantum Entanglement: A step towards Quantum Security

Scientists from S. N. Bose National Centre for Basic Sciences (SNBNCBS), Kolkata, an autonomous institute of the Department of Science and Technology have developed a novel protocol to find out whether a pair of electrons is in an entangled state so that they can be safely used as resources for facilitating quantum information processing tasks. The protocol has been developed through theoretical and experimental analysis.

Quantum entanglement is one of the peculiarities of quantum mechanics, which makes phenomena such as quantum teleportation and super-dense coding possible. It is the physical phenomenon that occurs when a pair or group of particles is generated, interact, in a way such that the quantum state of each particle of the pair or group cannot be described independently of the state of the others. Entangled states are key resources to facilitate many quantum information processing tasks and quantum cryptographic protocols.

However, entanglement is fragile and is easily lost during the transit of photons through the environment. Hence it is extremely important to know whether a pair of photons is entangled, in order to use them as resource. Verification of entanglement requires the use of measurement devices, but such devices may be hacked or compromised by eavesdroppers. Device-independent self-testing (DIST) is a method that can be used in order to overcome such a possibility.

This method enables the verification of entanglement in an unknown quantum state of two photons without having direct access to the state, or complete trust in the measurement devices. The theory relies on the application of the quantum uncertainty principle while implementing full device independence is a difficult task. In several practical situations, one of the parties may be fully trusted, whereas, the other may not be trusted like in the case of server-client relationship in banking transactions. For such situations, quantum information theory enables one-sided DIST (1sDIST).

In the protocol published in Physical Review A, Dr Archan S. Majumdar from SNBNCBS and his team, the theoretical idea is based on applying the fine-grained uncertainty relation to perform quantum steering. This idea has been successfully implemented experimentally by his team in collaboration with a group in Beijing Computational Science Research Centre, and Key Laboratory of Quantum Information, Hefei. The experiment uses an all-optical set-up in which entangled pairs of photons are created by laser light on Beta barium borate (BBO) crystals, a nonlinear optical crystal, used as laser crystal. The team used Bob as the trusted party and Alice as untrusted, to verify that the pair of photons they share is entangled.

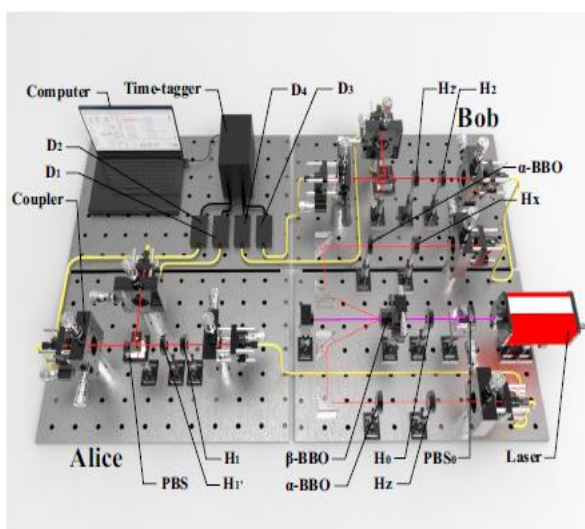


Figure: Representation of the experimental model

In a single run of their experiment, one photon goes to Alice's lab (bottom left), and another to Bob's lab (top right). They implemented several optical operations using beam-splitters, phase-shifters, and quantum gate operations before the photons were detected. Using the detection statistics, the team not only certified the presence of entanglement but also determined the magnitude of entanglement in the photon pairs with minimum error.

The team concluded that the entangled pairs of photons generated by the laser and BBO crystals can be reliably used to perform secure communication tasks.

Publication link: <https://doi.org/10.1103.PhysRevA.98.022311>,
<https://doi.org/10.1103.PhysRevA.101.020301>

For more details, Archan S. Majumdar (archan@bose.res.in) can be contacted.