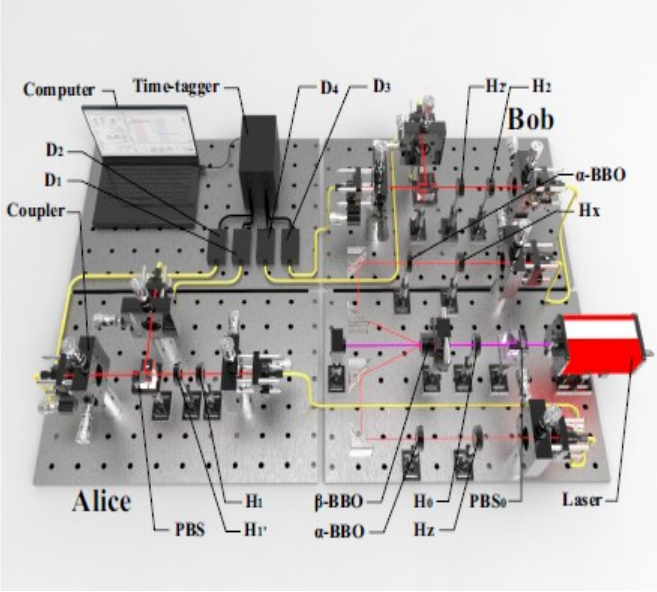
Certifying Quantum Entanglement: A step towards Quantum Security

[https://doi.org/10.1103.PhysRevA.98.022311]
[https://doi.org/10.1103.PhysRevA.101.020301]

Archan S. Majumdar
archan@bose.res.in
S. N. Bose National Centre for Basic Sciences, Kolkata

Nearly hundred years after its discovery, quantum mechanics has reached an important threshold. Today, the laws of quantum physics play an essential role in safeguarding our ability to communicate securely. All communication activities ranging from financial transactions, data exchange and online education to personal emails, all would be untrustworthy in the absence of guaranteed protection from hackers and fraudsters. During the last two decades, it has been realized that two inherent properties possessed by fundamental particles such as photons, can indeed guarantee the privacy of communication using such information carriers. The application of quantum principles in storage, transfer and manipulation of information using these two properties, *viz.*, superposition and entanglement, has opened up a whole new branch of physics called Quantum Information Science.

Quantum information theory predicts the possibility of certain tasks which cannot be realized using laws of classical physics. Primary among them are the processes of quantum teleportation, quantum computation and quantum cryptography. Some of these tasks can be accomplished through the creation of quantum entanglement between the states of two or more particles such as photons. Entanglement is a resource which enables many useful tasks of quantum information processing. However, entanglement is fragile, and is easily lost during the transit of photons through the environment. It is hence, 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. In order to overcome such a possibility, device independent entanglement verification, or device independent self-testing has been proposed recently.



Device-independent self-testing (DIST) 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 application of the quantum uncertainty principle. Implementing full device independence is a difficult task. Inseveral practical situations, one of the parties may be fully trusted, whereas, the other is untrusted, for example, the server-client relationship in banking transactions. For such situations, quantum information theory enables one-sided DIST (1sDIST). See, the figure where Bob is the trusted party and Alice is untrusted, and we have to verify that the pair of photons they share is entangled.

In our work we have formulated the first protocol (both theory and experiment) for 1sDIST. The theoretical idea is based on applying the fine-grained uncertainty relation to perform quantum steering [Phys. Rev. A 98, 022311 (2018)]. This idea has been successfully implemented

experimentally by us in collaboration with a group in Beijing Computational Science Research Centre, and Key Laboratory of Quantum Information, Hefei [Phys. Rev. A 101, 020301(R) (2020)]. The experiment uses an all optical set-up (see the figure), in which entangled pairs of photons are created by laser light on BBO crystals. In a single run of the experiment, one photon goes to Alice's lab (bottom left), and another to Bob's lab (top right). Next, several optical operations using beam-splitters, phase-shifters, and quantum gate operations are implemented before the photons are detected. Using the detection statistics, we are able to not only certify the presence of entanglement, but also determine the magnitude of entanglement in the photon pairs with minimum error. We can thus conclude that the entangled pairs of photons generated by the laser and BBO crystals can be reliably used to perform secure communication tasks.

DOI: 10.1103/PhysRevA.101.020301