Warszawa, 01.09.2022

Shubhayan Sarkar
Centrum Fizyki Teoretycznej PAN
Aleja Lotników 32/46
02-668 Warszawa

Summary of the doctoral thesis

"Certification of entangled quantum states and quantum measurements in Hilbert spaces of arbitrary dimension"

The emergence of quantum theory at the beginning of 20-*th* century has changed our view of the microscopic world and has led to applications such as quantum teleportation, quantum random number generation and quantum computation to name a few, that could never have been realised using classical systems. One such application that has attracted considerable attention lately is device-independent (DI) certification of composite quantum systems. The basic idea behind it is to treat a given device as a black box that given some input generates an output, and then to verify whether it works as expected by only studying the statistics generated by this device. The novelty of these certification schemes lies in the fact that one can almost completely characterise the device (up to certain equivalences) under minimal physically well-motivated assumptions such as that the device is described using quantum theory. The resource required in most of these certification schemes is quantum non-locality.

A lot of work has recently been put into finding DI certification schemes for composite quantum systems. Most of them are however restricted to lower-dimensional systems, in particular two-qubit states. In this thesis, we consider the problem of designing general DI schemes that apply to composite quantum systems of arbitrary local dimensions. First, we construct a fully DI certification scheme, also known as self-testing, that allows us to certify generalised Greenberger-Horne-Zeilinger (GHZ) states of arbitrary local dimension shared among any number of parties from the maximal violation of a certain family of Bell inequalities, for two parties, the generalised GHZ state represents the two-qudit maximally entangled state. Importantly, this is the first instance where such states can be certified using only two measurements per party which is in fact the minimal number of measurements required to observe quantum non-locality.

While a substantial progress has been recently made in designing device-independent certification schemes, most of these schemes are concerned with entangled quantum states. At the same time the problem of certification of quantum measurements remains largely unexplored. In particular, a general scheme allowing one to certify any set of incompatible quantum measurements has not been proposed so far. As designing such a scheme within the DI setting is certainly a difficult task, here we consider a relaxation of the Bell scenario known as the one-sided device-independent (1SDI) scenario. In this scenario, we have an additional assumption that one of the parties is trusted and the measurements performed by this party are known. We propose a scheme for certification of a general class of projective measurements, termed here "genuinely incompatible". To this end, we construct a family of steering inequalities that are maximally violated by any set of genuinely incompatible measurements. Interestingly, mutually unbiased bases belong to this class of measurements. Finally, in the 1SDI scenario, we construct a family of steering inequalities, whose maximal violation can be used to certify any pure entangled bipartite state using the minimal number of two measurements per observer. Building on this result, we then provide a method to certify any rank-one extremal measurement, including non-projective measurements on the untrusted side.

Interestingly, self-testing of entangled states and measurements can be harnessed to propose schemes to certify that the outcomes of measurements performed on quantum states are perfectly random in the sense that they can not be predicted by an external party. This makes our scheme suitable for quantum cryptographic tasks. We first show that one can generate randomness in a fully DI way using projective measurements from composite quantum states of arbitrary local dimension. Later in the 1SDI scenario, we construct a scheme to certify the optimal amount of randomness that can be generated using a quantum system of any dimension and non-projective extremal measurements, which is twice the amount one can generate using projective measurements.

Shubhayan Sarkar.

Shubhayan Sarkar