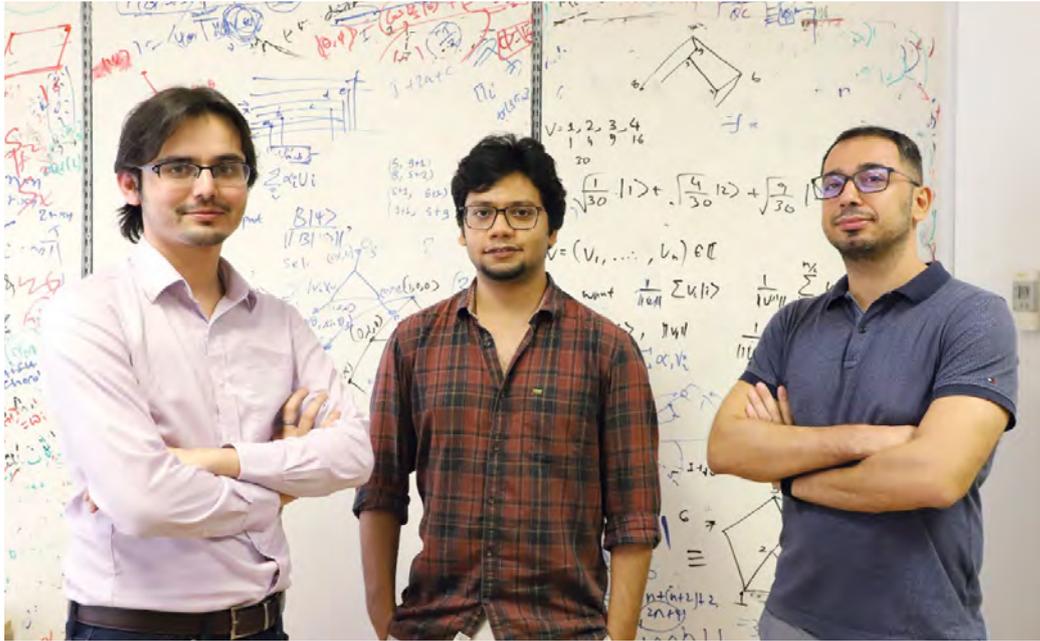


Scheme will Certify Solo Quantum Devices

XIN-YI PHUAH



Caption for picture: With their new graph-based approach, researchers (from left) Kishor Bharti, Maharshi Ray, Antonios Varvitsiotis and their colleagues have extended the notion of self-testing to local quantum systems.

CQT researchers and their colleagues find a way to do self-testing for single quantum devices, when previous schemes worked only for pairs

Suppose that Alice and Bob buy quantum devices from an untrusted supplier. Researchers already knew that Alice and Bob could make measurements on pairs of devices to certify the devices' quantum behaviour. Now CQT researchers and their collaborators have come up with a way to test single devices too. Their findings are published on 26 June 2019 in *Physical Review Letters*.

Certifying that a device has its promised quantum powers relies on 'self-testing' of their quantum states, with potential applications in technologies including random number generation and quantum cryptography. The idea of self-testing was first introduced for 'Bell scenarios', where components in the devices of Alice and Bob are entangled. When two quantum objects are entangled,

an action performed on one will affect the outcome of an action performed on the other. The physicist John Bell showed in the 1960s that such entangled states give rise to 'two-party measurement statistics' which cannot be faked by any non-quantum systems.

Given the critical role these statistics played in previous self-testing schemes, for a long time it was not known if the idea of self-testing could be applied to a single party. In other words, can Alice self-test her quantum device without Bob?

CQT's Kishor Bharti and his colleagues have shown that Alice can go for it alone. Kishor, a CQT PhD student, worked on the problem with colleagues Maharshi Ray, Naqeeb Ahmad Warsi and LeongChuan Kwek from CQT; Antonios Varvitsiotis from the NUS Department of Electrical and Computer Engineering; and Adán Cabello from the Universidad de Sevilla, Spain.

In the paper “Robust self-testing of quantum systems via non-contextuality inequalities”, the team provides a novel scheme to self-test local quantum systems that does not use entanglement.

“Entanglement is considered a costly resource for quantum information processing tasks,” says Kishor, who is first author of the paper. “Thus, certifying a quantum device with less entanglement is always favourable.”

Instead of entanglement, the scheme makes use of a quantum property known as contextuality. What contextuality means is that the result of a measurement made on the quantum system depends on the other measurements made together with that particular measurement.

In addition to contextuality, the work leverages on techniques from mathematical optimisation, a modelling tool used extensively in science and engineering. The optimisation model used in the proposed scheme is semidefinite programming (SDP).

The scheme also makes a few key assumptions: the quantum device has bounded memory, and the measurements going on inside the device follow some structure dictated by an ‘odd cycle graph’. That means considering the measurements as a pattern of nodes and edges. The nodes are individual events, or the measurements that are made on the quantum device. Two nodes are connected by an edge if they are exclusive—meaning that if one happens, the other cannot happen. What gives the

odd cycle graph its name is that it has an odd number of nodes and edges, and the graph starts and ends at the same point.

The property of having an odd cycle graph structure could be designed into devices to make such self-testing possible. “In future, one can demand such a structure in a quantum computer to verify if it is indeed a quantum computer,” says Kishor.

A given set of measurements will have a target value, the Lovász theta number for that particular scenario. Matching this targeted value in self-testing means that the device has passed the test. Alice can certify that her device is indeed the promised quantum device.

Importantly, the self-testing scheme is robust one. Robustness is paramount in making the scheme practical for real world scenarios where devices might not always have perfect performance. If the quantum device achieves something close to but falls short of the target number, the device would still be useful. In other words, it might not be the best-performing device there is, but Alice would still be able to use her quantum device with confidence.

The team found the results of their new ‘graph-based’ approach rewarding. “It is the first time that graph theory is used together with self-testing,” says Kishor. “We went into new territory and saw interesting things. It was really satisfying.”