Device-independent algorithms with superconducting circuits

Anatoly Kulikov[1]
Simon Storz[1], Josua Schär[1], Martin Sandfuchs[1], Ramona Wolf[1], Florence Berterottiere[1], Christoph Hellings[1], Victor Barizien[2], Xavier Valcarce[2], Jean-Daniel Bancal[2], Nicolas Sangouard[2], Renato Renner[1], Andreas Wallraff[1]

[1]ETH Zurich, Switzerland; [2]Université Paris-Saclay, CEA, CNRS, France

akulikov@phys.ethz.ch

The successful realization of loophole-free Bell tests has settled an 80-year-long debate on the foundations of quantum mechanics and manifested that non-locality is an inherent property of quantum physics and could be considered a useful resource for quantum information processing. With applications envisaged more than three decades ago[1], non-locality forms a basis for *device-independent* algorithms, especially suited for quantum key distribution, generation of certified randomness or self-verification of untrusted devices. In such protocols, one explicitly discards the requirements of the exact knowledge of the employed device, and assumptions of its strict correspondence to a theoretical model. Instead, it is possible to certify the output of a given protocol based on fundamental physical principles.
In this talk, I will present an experimental implementation of two such device-independent algorithms using a circuit QED platform based on superconducting circuits in a setup like the one used for the recently reported loophole-free Bell inequality violation[2], see Fig. 1. Entangling a system composed of two superconducting qubits separated by 30 meters, we perform self-testing of both the generated Bell state and the measurement fidelity in a device-independent manner. In a second experiment, we turn to the omnipresent task of generating high-quality randomness and realize randomness amplification and privatization[3]. Specifically, using the resource of non-local entanglement certified by a loophole-free violation of a Bell inequality, and a public, imperfect source of randomness, we obtain near-perfect private randomness as an output.
Both protocols mark a step towards secure quantum communication and information processing and demonstrate applications not attainable using classical information processing systems.

Figures

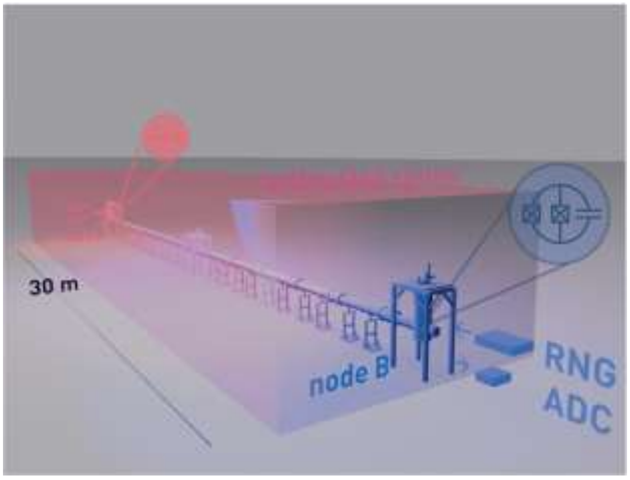

Figure 1: Illustration of the experimental setup used to entangle superconducting qubits across a distance of 30 meters. At each of the two nodes A and B a superconducting qubit is operated in a dilution refrigerator. The two nodes are connected via a cryogenic quantum link housing a 30-meter-long microwave waveguide to allow for photon exchange and entanglement distribution. Each node operates a trusted random number generator (RNG) and a measurement signal detection device (analog-to-digital converter, ADC).

References

[1] A. Ekert, Phys. Rev. Lett., 67:661, 1991
[2] S. Storz et al, Nature 617:265–270, 2023
[3] R. Colbeck and R. Renner, Nat. Phys., 8:450, 2012