Measurement-device-independent randomness generation with arbitrary states

Felix Bischof, Hermann Kampermann, and Dagmar Bruß

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany

Random numbers are a fundamental resource for many information-theoretical tasks, in particular classical and quantum cryptography. Here, standard protocols require that the communicating parties have access to bit strings that are unknown and uncorrelated to any other party, including a potential eavesdropper; a property which is called true randomness [1], or private randomness [2].

In nature, private randomness is made possible by the intrinsic unpredictability of quantum measurements: even if the whole system is known, outcomes cannot be predicted with certainty. Yet, even in quantum mechanics, true randomness cannot be shown without further assumptions. This is because realistic settings always exhibit a mixture of classical and true randomness, where the former must be attributed to the malicious influence of an eavesdropper. The challenge remains in separating and quantifying these types of randomness, while keeping the assumptions experimentally viable.

Previous work has addressed the dependence of the randomness generation rate on the level of control of the devices [3]. There exist fully device-independent schemes that are unpractical because of the required high detector efficiency needed to violate Bell inequalities, and different kinds of semi-device independent schemes.

Inspired by the concept of measurement-device-independent quantum cryptography, put forward by [4], we have investigated measurement-device-independent (MDI) randomness generation to generate private random numbers with few assumptions. In this scheme, trusted sending devices produce quantum states inside a secure laboratory. Upon receiving the signals, an uncharacterized measurement apparatus outputs classical bits, the raw random numbers. The observed measurement statistics is then used to quantify the amount of true randomness, independent of the inner working of the measurement device.

While results for MDI randomness generation have been obtained for special cases, e.g. [5], we present a general framework to quantify the measurement-device independent randomness generation rate for any implementation: arbitrary sent states, and detectors with an arbitrary number of outcomes are possible. The theoretical analysis is based on showing that this general setting can be cast into the form of a semidefinite program, which can be solved by numerical methods. The result is then used to derive simple and realistic implementations that yield high randomness generation rates, even for noisy detectors.

References

[1] D. Frauchiger, R. Renner, and M. Troyer. True randomness from realistic quantum devices (2013). *arXiv preprint arXiv:1311.4547*.

[2] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[3] Y. Z. Law et al. Quantum randomness extraction for various levels of characterization of the devices. *Journal of Physics A:*, 47(42):424028, 2014.

[4] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[5] Z. Cao, H. Zhou, and X. Ma. Loss-tolerant measurement-device-independent quantum random number generation. *New Journal of Physics*, 17(12):125011, 2015.