A Self-Testing Quantum Random Number Generator

Tommaso Lunghi¹, Jonatan Bohr Brask², Charles Ci Wen Lim¹, Quentin Lavigne¹,
Joseph Bowles², Anthony Martin¹, Hugo Zbinden¹, and Nicolas Brunner²

¹. Group of Applied Physics, Université de Genève, 1211 Genève, Switzerland
². Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland

The generation of random numbers is a task of paramount importance in modern science. A central problem for both classical and quantum randomness generation is to estimate the entropy of the data generated by a given device. Here we present a protocol for self-testing quantum random number generation, in which the user can monitor the entropy in real time. Based on a few general assumptions, our protocol guarantees continuous generation of high quality randomness, without the need for a detailed characterization of the devices. Using heralded single-photon generation based on spontaneous parametric down conversion, we have implemented our protocol and illustrated its self-testing capacity. Our work thus provides a practical approach to quantum randomness generation in a scenario of trusted but error-prone devices. It has been published in [1].

References