Certified random numbers from quantum steering

Dominick J. Joch[a], Sergei Slussarenko[a], Yuanlong Wang[a], Alex Pepper[a], Shouyi Xie[b], Bin–Bin Xu[b], Ian R. Berkman[b], Sven Rogge[b], and Geoff J. Pryde[a]

[a]*Centre for Quantum Dynamics and Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane, Queensland 4111, Australia*

[b]*Centre for Quantum Computation and Communication Technology, School of Physics, The University of New South Wales, Sydney, NSW 2052, Australia*

Genuine randomness is a central resource for cryptography and a multitude of other applications. Cryptographic keys are commonly produced by pseudo-random number generation (RNG), which is deterministic, and dependent on an adversary lacking the computing power to guess the seed. Quantum phenomena possess intrinsic randomness, making quantum-RNG (QRNG) the most appealing avenue for secure randomness [1,2]. However, naïve approaches rely on strong assumptions about the physical devices, making them susceptible to adversarial exploitation. By exploiting quantum nonlocality, some QRNG schemes have a large degree of device independence (DI), and the best possible levels of security [1]. Full DI-QRNG is highly challenging experimentally, which motivates partially-DI schemes that trade some additional assumptions for significant advantages in ease of implementation and can therefore become commercially feasible sooner.

Our work implements such a scheme—based on the quantum steering task—that is more robust to loss and has greater noise tolerance than DI-QRNG protocols and superior security to trusted-device and many other partially-DI approaches [3]. We use single photons to implement the protocol and demonstrate randomness expansion and the experimental and security advantages [4]. We create photon pairs by spontaneous parametric downconversion to prepare states that have a high fidelity of 0.9933 ± 0.0005 with the maximally entangled singlet Bell state. We apply a quantum-proof randomness extractor to obtain the final certified random sequence of bits. This scheme allows us to certify randomness below the efficiencies required for DI-QRNG (see Figure 1). Our scheme can be refined to serve as a viable randomness beacon and is an important step toward improved security of public randomness sources and private randomness for cryptographic purposes.

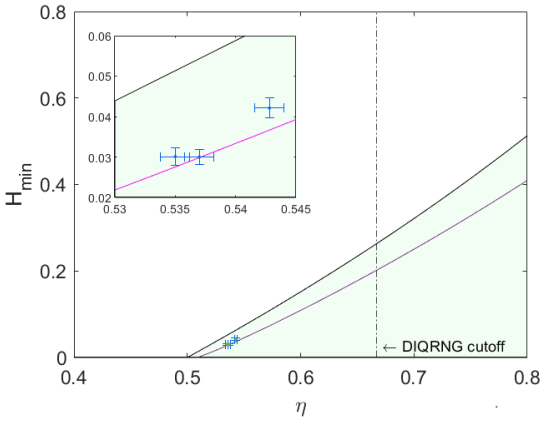

Figure 1: Randomness certified via quantum steering and quantified using min-entropy as a function of efficiency of the untrusted channel.

[1] Masanes, L. & Acín, A. Nature 213–219 (2016).

[2] Herrero-Collantes, M. & Garcia-Escartin, J. C. Rev. Mod. Phys. 89, 015004(2017).

[3] Passaro, E., Cavalcanti, D., Skrzypczyk, P. & Acín, A. New J. Phys. 17,113010 (2015).

[4] Joch, D. J. *et al.* (2021). Preprint at https://arxiv.org/abs/2111.09506.