Semi-device-independent quantum randomness generation

Thomas Van Himbeeck,[1,2] Stefano Pironio,[1,2] and Jonatan Bohr Brask[3]

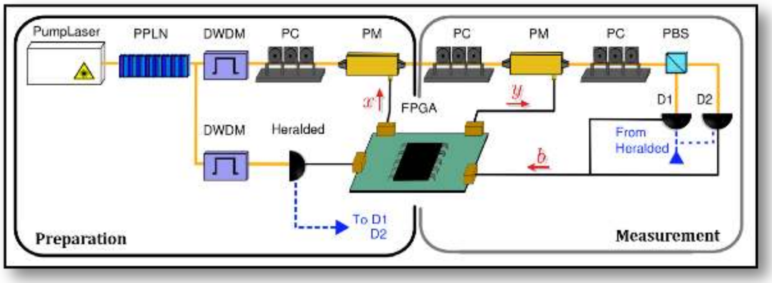
[1] *Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium*
[2] *Centre for Quantum Information and Communication, Université libre de Bruxelles (ULB), Belgium*
[3] *Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*

Exploiting quantum systems enables strong security in information processing, e.g. for tasks such as random number generation and cryptography. This can be done under different levels of trust in the devices used. In a completely device dependent scenario, security is analysed based on a full quantum description. Remarkably, security can also be certified in a completely device independent scenario, were the inner workings of the devices are unknown, through the violation of a Bell inequality. The device-dependent approach generally gives high rates, but a full characterisation of the devices may be difficult to obtain or verify, while the device-independent approach is technologically very challenging to implement at present, because it requires Bell inequality violation free of the detection loophole, leading to low rates. It is therefore interesting to explore intermediate regimes, to identify an optimal trade-off between ease of implementation and trust in the devices.

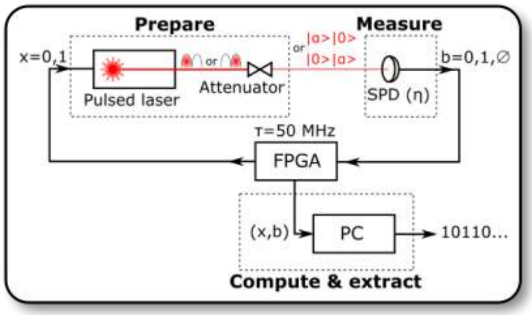
In this talk, we present a new approach [1] to semi device independence for prepare-and-measure protocols, and review two recent experiments realising semi-device-independent quantum random number generation. Previous schemes assumed a bound on the dimension of the Hilbert space characterizing the quantum carriers. Here, we propose instead to constrain the quantum carriers through a bound on the mean value of a well-chosen observable. This modified assumption is physically better motivated than a dimension bound and closer to the description of actual experiments. In particular, we consider quantum optical schemes where the source emits quantum states described in an infinite-dimensional Fock space and model our assumption as an upper bound on the average photon number in the emitted states

In the first part of the talk, we present the new framework in the simplest possible scenario, based on two energy-constrained state preparations and a two-outcome measurement. We find that there exist quantum correlations which cannot be reproduced by any classical model of the devices, and show how this enables generation of certified randomness. This opens the path to more sophisticated energy-constrained semi-device-independent quantum cryptography protocols, such as quantum key distribution.

In the second part of the talk, we review two recent implementations of semi-device-independent randomness generation. The protocols are based respectively on testing a dimension witness [2] (setup illustrated in Fig. 1a), in the spirit of previous approaches, and on unambiguous state discrimination [3] (setup illustrated in Fig. 1b), which is similar in spirit to the new framework introduced in the first part (although different from it). Both implementations allow the user to monitor the entropy in real time. The latter experiment achieved a 16 MHz random bit rate, comparable to commercial quantum random number generators which operate in the device-dependent setting.



(a) Experimental setup from [2].



(b) Experimental setup from [3].

[1] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, arXiv [quant-ph] , 1612.06828 (2016).

[2] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).

[3] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Applied **7**, 054018 (2017).