Toward the generation of Bell certified randomness using photons

Jean-Daniel Bancal[1], Siddarth Koduru Josh[1], Chen Ming Chia[1], Alessandro Cere[1], Lana Sheridan[1], Valerio Scarani[1,2], Christian Kurtsiefer[1,2]

[1] Centre for Quantum Technologies, National University of Singapore, Singapore
[2] Department of Physics, National University of Singapore, Singapore

April 20, 2013

Randomness plays a fundamental role in the security of cryptographic protocols, as well as in the accuracy of numerical simulations. A system that violates a Bell inequality with a closed detection loophole and clear separation between its subsystems can be used to generate random numbers that are certified, i.e. both secure and truly random [1]. Given the high rate at which pairs of entangled photons can be created, they constitute promising candidates for practical certified randomness generation [2].

We present our progresses toward an experimental demonstration of a violation of the CHSH Bell inequality closing the detection loophole with near-infrared photons.

To evalutate the CHSH expression despite the stochastic nature of our source, we introduce a binning strategy for the detection events. This allows us to describe our setup within the usual device-independent framework and thus to use it for the generation of certified randomness.

We also introduce an algorithm that takes into account the full statistics of the observed correlations in order to quantify the amount of usable private randomness that can be extracted experimentally with detectors of finite efficiency. In the case of the presented experiment, this provides a tighter bound than the one that can be deduced using only the observed value of the CHSH operator. This larger amount of randomness that can be extracted from the observed full statistics is witnessed by a new Bell inequality, inequivalent to CHSH.

The source we use is based on a periodically poled KTP crystal, pumped by UV light in two opposite directions, inserted in a Sagnac-like configuration [3] (see Figure 1). It generates photons pairs ar 810nm with an adjustable degree of entanglement in polarization.

We use two high detection efficiency (>95%) transition edge sensors

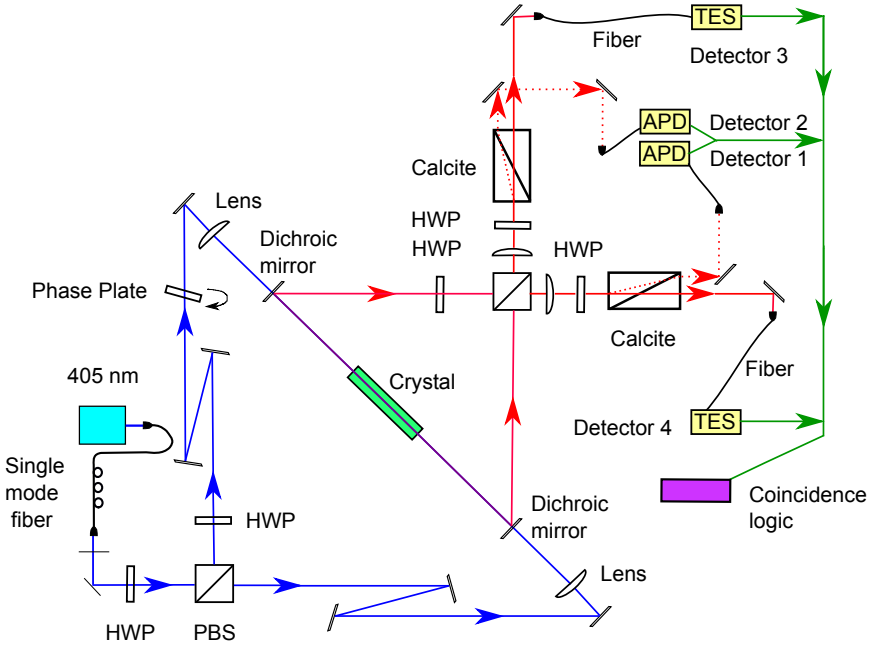

Figure 1: Experimental setup for certified randomness generation.

(TES) [4]. Including all losses we measure an overall pair detection efficiency larger than 70%, which is sufficient to close the detection loophole.

The setup presented can be extended to close the remaining loopholes to obtain a complete loophole free violation of the CHSH Bell inequality.

References

[1] S. Pironio et al., Nature **464**, 1021 (2010).

[2] A. Ling, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **77**, 043834 (2008).

[3] M. Fiorentino et al., Phys. Rev. A **69**, 041801 (2004).

[4] A. E. Lita, A. J. Miller, and S. W. Nam Opt. Express **16**, 3032 (2008).