Toward the generation of Bell certified randomness using photons

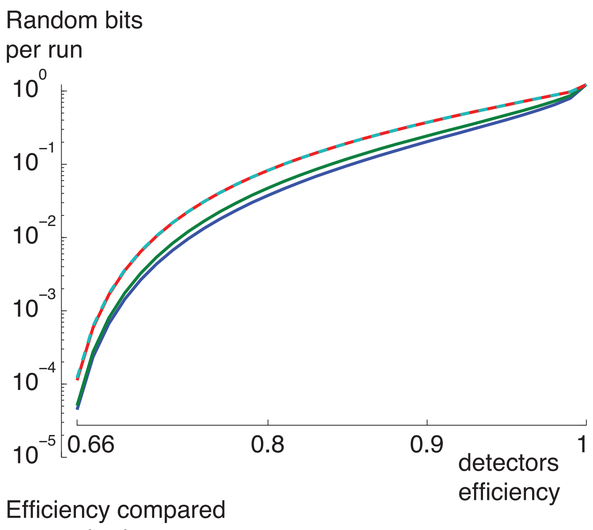
Siddarth Koduru Joshi[1], Chia Chen Ming[1], Alessandro Cerè[1], Jean-Daniel Bancal[1], Lana Sheridan[1], Valerio Scarani[1,2], Christian Kurtsiefer[1,2]

[1]Centre for Quantum Technologies, National University of Singapore, Singapore 117543
[2]Department of Physics, National University of Singapore, Singapore 117542

Introduction

Sources of true randomness have numerous applications, be it in algorithms, gambling or cryptography [1]. However, their unpredictability is typically difficult to certify since they may be correlated to external variables, and access to those other variable could render their behavior predictable. Therefore, there is strong motivation for developing sources of randomness that can be certified as being uncorrelated to any outside process or variable, i.e. sources of private randomness. Quantum physics offers this opportunity by means of violation of a Bell inequality. The recent technological advancements for high efficiency infrared photons detection, combined with a high efficiency photon pair source and a fast electro-optic polarization switch, opens the possibility of a loophole free experimental violation of the Bell inequality, paving the way for the realization of source of certified randomness.

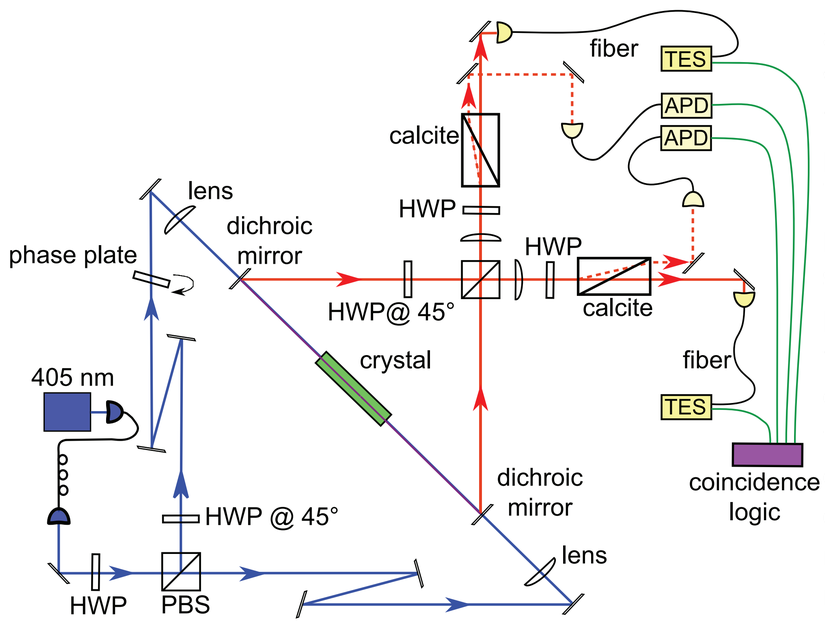
Generated certified randomness with real detectors



A violation of a Bell inequality ensures the presence of genuine private randomness in the measured correlation [2,3]. This violation can also be observed in the case of non-ideal detection efficiency, as long as the overall efficiency is larger than $2/3$ and the state and measurement basis are chosen appropriately [4]. It is possible to estimate a lower bound for the amount of certified randomness than can be generated as a function of the detection efficiency η and until now this bound was based only on the correlation statistics and assuming a non-uniform choice of the Bell basis as optimal strategy. We have improved the estimation of this lower bound by including the full measured statistic generated and assuming a uniform distribution for the choice of the measurement basis.

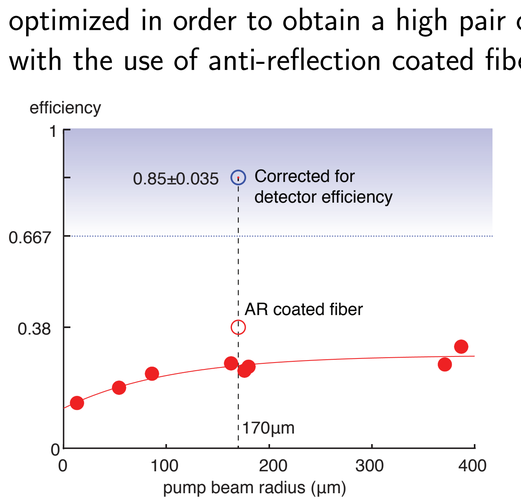
Source of entangled photon pairs

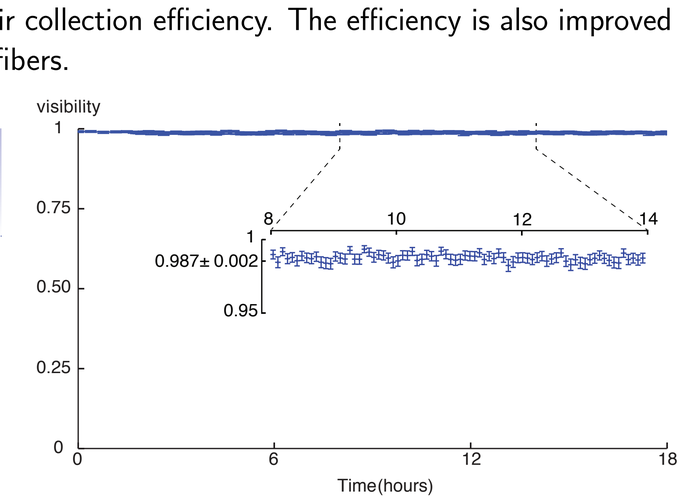
A critical resource for a Bell test experiment is a source for entangled photon pairs that allows a high pair detection efficiency. We use the entanglement between the horizontal (H) and vertical (V) polarization modes.



The source is based on a Sagnac-like geometry where two independent type-II down conversion processes are combined [5]. The two down conversion processes happen in the same crystal, a periodically poled KTP, temperature tuned for optimal collinear phase matching for 405 nm→810 nm. The crystal is pumped in two different directions and the resulting down-converted modes are combined in a polarizing beam splitter.

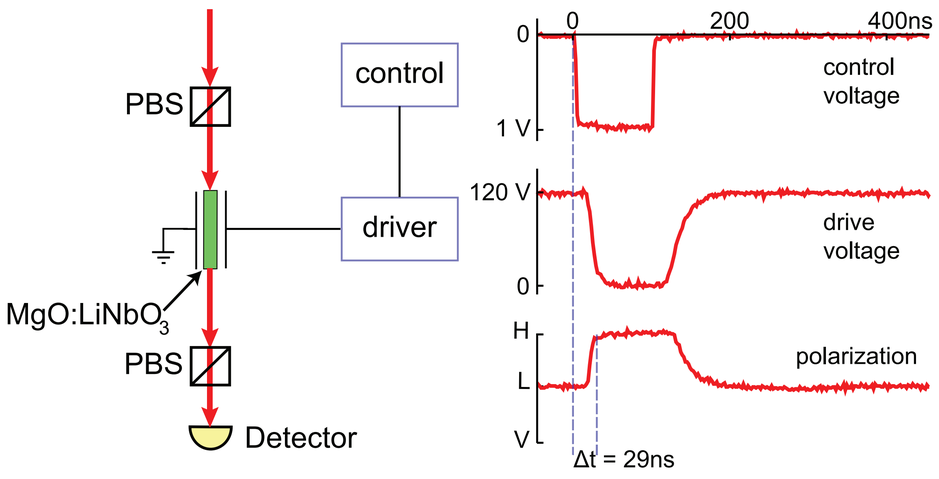
It is possible to generate the non-maximally entangled state ($|\psi\rangle = \cos\theta|HV\rangle + e^{i\phi}\sin\theta|VH\rangle$), with θ and ϕ optimized to provide the maximum possible violation according to [4]. The balance between the two arms of the pump controls θ while their relative phase controls ϕ. The phase ϕ is actively stabilized by a feedback lock that provides the long term stability necessary for long data acquisition. The pump and collection modes are optimized in order to obtain a high pair collection efficiency. The efficiency is also improved with the use of anti-reflection coated fibers.



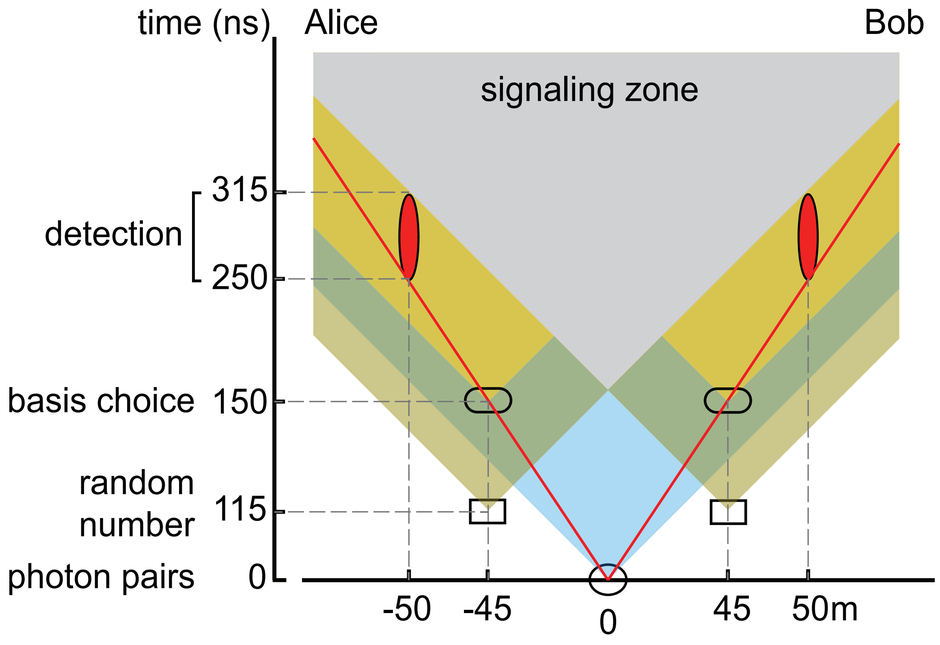


Timing and distances

In order to close the locality loophole, the basis choice and the detection need to be separated in space and time to exclude any possibility of communication. The minimum distance between the basis choice and the detection from the source and between each other depends on how fast those processes happen. To minimize this distance, and the associated losses, we have developed a fast polarization rotation based on an electro-optical modulator.

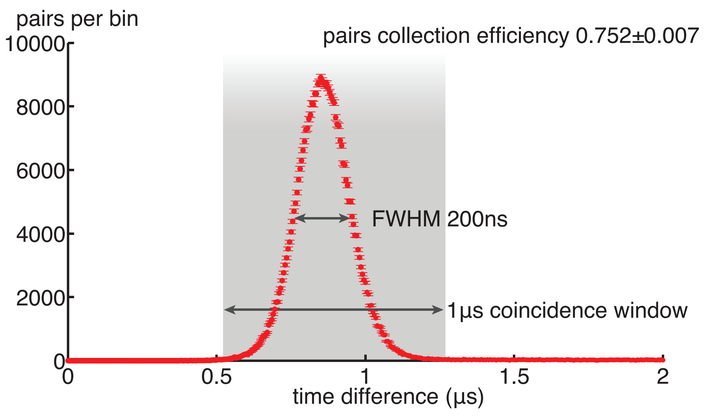


The locality conditions are resumed in a space-time diagram.
In red the generated photon in fiber propagation.



Detection efficiency

In order to close the detection loophole we use two transition-edge sensors (TES). These detectors can provide a detection efficiency above 0.95 in the single photon regime [6]. We estimated their quantum efficiency using one arm of the source (without the polarizers).



We can use this measurement to estimate the overall efficiency to see how it compares to the Eberhard limit.

		η
pairs generation and collection		0.85
polarization projection		0.97
fiber transmission	intrinsic	0.99
	splices	0.94
detection		0.93
Total		0.71>0.667

References

[1] S. Vadhan. Pseudorandomness, volume 7 of Foundations and Trends in Theoretical Computer Science. Now Publishers (2012).
[2] S. Pironio, et al., Nature, **464**,1021 (2010).
[3] R. Colbeck. "Quantum And Relativistic Protocols For Secure Multi-Party Computation". PhD thesis, University of Cambridge (2006). arXiv:0911.3814.
[4] P.H. Eberhard, Phys Rev. A **47**, R747 (1993)
[5] M. Fiorentino, F.N.C. Wong, J.H. Shapiro, Phys. Rev. A **69**, 041801 (2004)
[6] A.E. Lita, A.J. Miller, and Sae Woo Nam, Opt. Express **16**,3032 (2008)