Certified randomness in tight space

Presenting Author: Boris Bourdoncle[1]
Co-Authors: Andreas Fyrillas[1], Alexandre Maïnos[1,2], Pierre-Emmanuel Emeriau[1], Kayleigh Start[1], Nico Margaria[1], Martina Morassi[3], Aristide Lemaître[3], Isabelle Sagnes[3], Petr Stepanov[1], Thi Huong Au[1], Sébastien Boissier[1], Niccolo Somaschi[1], Nicolas Maring[1], Nadia Belabas[3], Shane Mansfield[1]
[1]Quandela, 7 rue Léonard de Vinci, 91300 Massy, France
[2]Quantum Engineering Technology Labs, University of Bristol, BS81FD Bristol, UK
[3]Université Paris-Saclay, CNRS, Centre de Nanosciences et de nanotechnologies, 91120 Palaiseau, France
boris.bourdoncle@quandela.com

Reliable randomness is a core ingredient in algorithms, simulation and cryptography. The outcomes of measurements on entangled quantum states can violate Bell inequalities [1], thus guaranteeing their intrinsic randomness, which constitutes the basis for certified randomness generation [2]. However, this certification requires several spacelike separated devices, making it unfit for a compact apparatus [3]. Here we provide a general method for certified randomness generation on a small-scale application-ready device and perform an integrated photonic demonstration combining a solid-state emitter and a reconfigurable glass chip. In contrast to most existing certification protocols, which in the absence of spacelike separation are vulnerable to loopholes inherent to realistic devices [4], the protocol we implement accounts for information leakage and is thus compatible with emerging compact scalable devices. We achieve the highest standard in randomness with a 2-qubit photonic device cut out for real-world applications. We demonstrate a 94.5-hour-long stabilized process harnessing a bright and stable single-photon quantum-dot based source, feeding into a reconfigurable photonic chip. Using the contextuality framework [5], we robustly certify the highest standard of private randomness generation, i.e. cryptographic security even in the presence of quantum side information. This is a prototype for the controlled alliance of quantum hardware and protocols to reconcile practical limitations and device-independent certification.

References

[1] N. Brunner *et al. Review of Modern Physics* **86** (2014) 419–478.
[2] S. Pironio *et al. Nature* **464** (2010) 1021–1024.
[3] L. Shalm *et al. Nature Physics* **17** (2021) 452–456
[4] Y. Liu *et al. Nature* **562** (2018) 548–551.
[5] S. Abramsky, A. Brandenburger. *New Journal of Physics* **13** (2011) 113036.

Figures

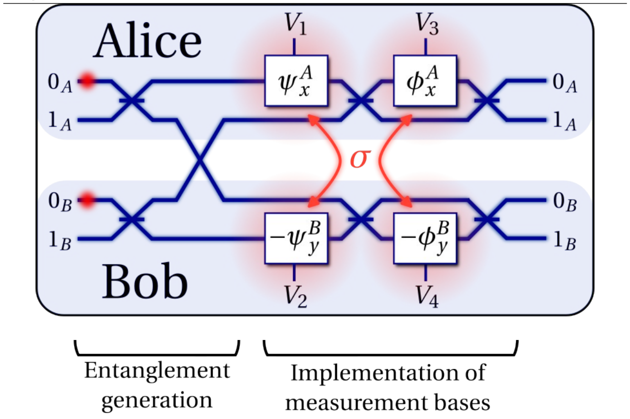

Figure 1: On-chip Bell inequality violation: two dual-rail encoded qubits are entangled via beamsplitters and a swap, and measured in different bases, selected via thermo-optic phase shifters. σ represents the information leakage e.g. crosstalk between the two parties.

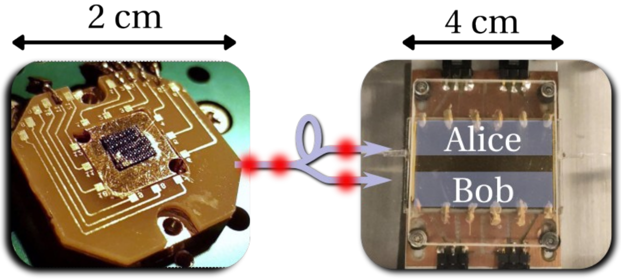

Figure 2: The quantum-dot device generates single photons sent to the photonic glass chip.