RAISE TAQS: Randomness expansion using a loophole-free Bell test

Krister Shalm (PI)
University of Colorado at Boulder

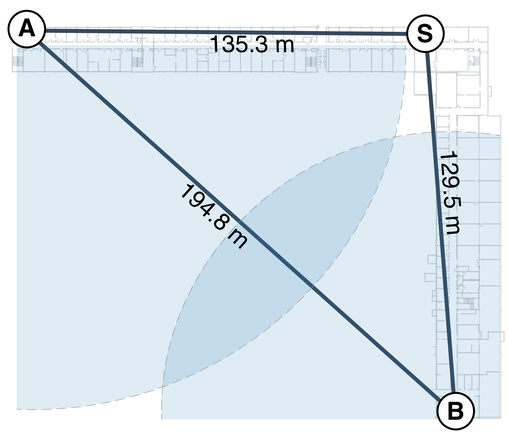
Paul Kwiat (CO-PI)
University of Illinois at Urbana-Champaign

Peter Bierhorst (CO-PI)
University of New Orleans

Overview

We are developing a compact quantum random number generator that uses quantum nonlocality. This is the only known way to produce random numbers whose quality can be certified. However, doing so requires satisfying a very strict set of parameters. Our current system involves multiple locations spread over hundreds of meters in a building. With this grant we are developing the next-generation certified random number generator that is two-orders of magnitude smaller, and will be capable of implementing advanced quantum protocols such as device-independent randomness expansion.

Our system can be thought of as a non-trivial Quantum 2.0 networked application. Entangled particles are distributed and operated on to produce a result not achievable by any other classical or quantum means.



University of Colorado Boulder
ILLINOIS
THE UNIVERSITY of NEW ORLEANS
Award Number: 1839223

Challenges

1. Quantum networked applications, such as this one, require faster modulators that are also low loss. We need optical switching of photons at rates > 100 MHz, but with losses less that 5%. These do not exist currently.

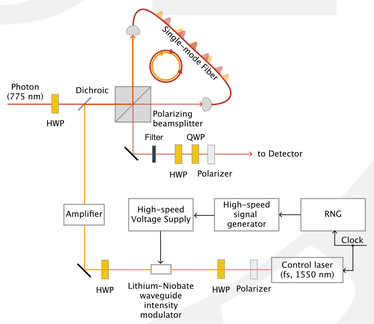
2. This area of research is less than 10 years old. A great deal of work remains on developing more efficient protocols.

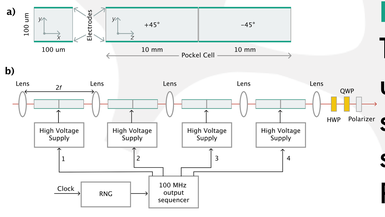
Approach

We are investigating all-optical switching using nonlinearities as well as new materials for a more traditional Pockels cell approach. Additionaly, we are developing new theoretical models that will allow us to generate randomness much faster.

Nonlinear Switching

Inside a Sagnac interferometer, counter-propagating polarization components of a single photon are coupled into a single-mode fiber. By modulating the intensity of the control laser, different polarization rotations can be performed.



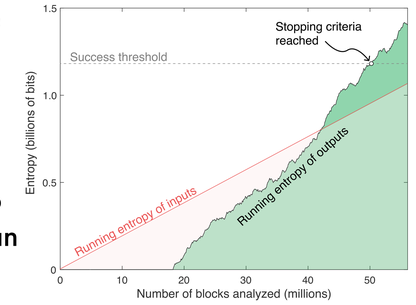


Pockels Cells

To achieve higher switching rates, up to 4 Pockels cells are used in series. A 100 MHz output sequencer drives a different Pockels cell each clock cycle.

Progress

Major protocol advances have enabled us to perform the first demonstration of randomness expansion using our current setup. From more than 100 hours of data, we were able to generate more random bits than were consumed. By moving to our next-generation tabletop setup we should be able to cut down our data taking time by 2-3 orders of magnitude.



Y. Zhang et al, *Certifying Quantum Randomness by Probability Estimation*, Phys. Rev. A **98**, 040304(R) (2018)

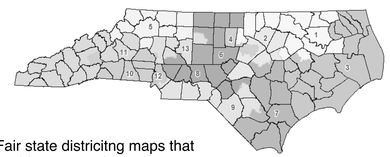
L. K. Shalm et al, *Device-independent Randomness Expansion with Entangled Photons*, arXiv:1912.11158 (2019)

We have also identified a promising new material for implementing Pockels Cells. The Kerr nonlinearity of this material is so strong that it will lower our voltage requirements by a factor of 100. This should allow us to exceed the 100 MHz requirements with less than 2% loss. The tabletop system is currently being constructed.

Broader Impacts

We are currently working on integrating our quantum source of randomness into a public randomness beacon. This will enable applications like video footage verification, resource allocation, and redistricting to occur in a more trustworthy and fair manner. Our project will lead to the first publicly available quantum 2.0 networked application.

Certified quantum random numbers



Fair state districitng maps that avoid gerrymandering.