Public Randomness Verification Using Quantum Path Encoding

R Piera[1], Y Kurochkin[1], J Singh[1], and J Grieve[1]

[1] *Quantum communications, TII, P.O.Box: 9639, Masdar City, Abu Dhabi, United Arab Emirates.*
Contact Phone: +971507759414
Contact Email: yury.kurochkin@tii.ae

Quantum random number generators (QRNG) are becoming one of the most widely used quantum applications. Useful advantage of QRNG is public verification based on quantum properties. It allows verifying the properties of bit strings without revealing the actual information about the application of random bits. We extract the entropy from the measurement of the superposition of multiple photon paths, which can also be analyzed as an entangled state after post-selection. In this work, we minimize the number of elements that can fail and lead to a perturbation of the properties of the quantum random sequence. As a result, we present a robust and verifiable QRNG.

We use the states proposed in the public randomness testing protocol as the resource [1]:

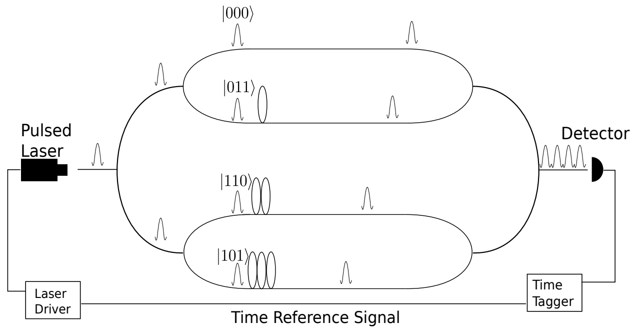

Figure 1: Optical path choice scheme to generate three bits connected by XOR condition

$$|\Phi\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \tag{1}$$

It can be prepared by the optical path superposition scheme shown in figure 1. Using a pulsed laser, beamsplitters and delay lines, we convert the path into a time window. Then we need only one click of the detector in four time windows. Under this condition, the state is postselected as described above when a single photon chooses the path. At the same time, the state can be considered as three bits connected by an XOR condition:

$$|\Phi\rangle = |0\rangle(\frac{|00\rangle + |11\rangle}{2}) + |1\rangle(\frac{|10\rangle + |01\rangle}{2}) \tag{2}$$

This happens because we use four states to encode eight bits. We use one of the sequences to announce for public verification and one of the other bit sequences for application. Component failure analysis shows that the locally used bit sequence still requires zero for unit statistics analysis. This function is a lightweight local computation compared to a comprehensive cloud randomness test. In this work, we assume a trusted device that can be compromised by the reasonable failure of a component. The use of a one single photon detector can protect against relatively rapid modulation of detector efficiency that may occur due to power supply effects. At the same time, failure of the passive beam splitter ratio can only occur on a large time scale, allowing us to control it on a reasonable statistical scale. With a pulse repetition rate of 3 MHz, we generate data blocks of 256 Mbytes, which we analyze with a public randomness test. After filtering out multiple clicks, we get 35 000 events per second, which we analyze with the Toeplitz extractor based on the public bitstring analysis and the epsilon parameter.

References

[1] J E. Jacak, W A. Jacak, W A Donderowicz and L Jacak, Sci. Rep. **10**, 164 (2020)