**Self-Correcting Quantum Random Number Generators for High Performance Computing**

Raphael Pooser and Ben Lawrie

Oak Ridge National Laboratory

lawriebj@ornl.gov

**Abstract**

Since the development of Monte Carlo simulations, independent and uniformly distributed sources of random numbers have been increasingly critical to the numerical modeling of highly coupled systems. Algorithmic pseudorandom number generators (pRNGs) have long since replaced tables of true random numbers for numerical modeling applications because of the speed and affordability of software based pRNGs. However, because pseudorandom numbers are inherently deterministic, simulations are constrained by the period of the pRNG, and dramatic systematic errors can emerge for some algorithms as a result of subtle correlations that cannot be seen by established randomness tests.

Quantum random number generators (QRNGs) offer the possibility of true randomness guaranteed by quantum mechanics. Most demonstrations of QRNGs to date have relied on the discrete quantum statistics of single photons at beam splitters, but the slow speed and high cost associated with generating and detecting single photons has limited the QRNG market. In addition, while QRNGs offer true randomness, they also exhibit non-uniform distributions that result in biased sampling. Software post-processing used to remove this bias further slow QRNGs. The self-correcting QRNG described here extracts random numbers from the vacuum field fluctuations encoded in the location of photons within a bright field of light, resulting in orders of magnitude improvement in the cost and speed of the QRNG relative to any QRNG based on single photons. Combining this continuous variable quantum optics approach to random number generation with continuous state characterization and quantum feedback control removes bias in real time, eliminating the requirement of post-processing and further improving the speed of the QRNG.