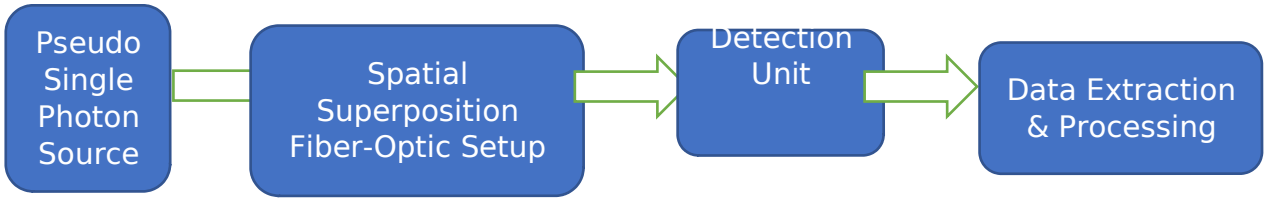
Quantum Random Number Generator (QRNG)

Random Number Generators have immense applications in a lot of areas like Key Generation, Cryptography, banking, automotive industry, security, etc. DRDO Young Scientist Laboratory for Quantum Technologies (DYSL–QT), Pune has developed Quantum Random Number Generator (QRNG) exploiting the principles of Quantum Physics to generate true randomness.

In the approach followed, the spatial superposition property of single photons in fibre–optic medium is used to generate random numbers. The whole architecture consists of the following sub–sections.



The generated single photons will be in a state of spatial superposition after passing through the fiber–optic setup which will subsequently be fed to a pair of detectors. Detector outputs will be used to generate the random data which will be processed further using the extraction and processing unit designed using FPGA.

This developed architecture–generated random numbers have been tested in–house using standard Test Suites such as NIST STS, Die–Harder, ENT, etc and have successfully passed all of them. Additionally, the data were certified by one of the sister–labs of DRDO and has undergone performance evaluation at another DRDO lab.