# Studying the effect of input states

## Introduction:

Information and communication security is crucial in the world we live in. Consequently, encryption methods are important. The degree of randomness utilized to create the key affects how strong it is. The strength of the key increases with entropy. Random numbers are crucial in the lottery industry, scientific simulations, genetics, and statistical sampling, in addition to cryptography. Therefore, Sources of random number generation are important. In the classical field, there are various methods that can generate random numbers, but the numbers generated in this way are pseudo-random and very susceptible to detection. Hence, having access to reliable random number generator tools is necessary.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that security can not be compromised. This procedure is known as quantum cryptography. The basic idea is to exploit the quantum mechanical principle that observation and measurement in general disturbs the system state being observed and causes the initial state of the system to collapse and part of its information is completely lost during the measurement. The intrinsic randomness of quantum physics makes quantum systems a good source of RNG(QRNG). One of the methods of generating random numbers is using boson sampling.

## Quantum Random Number Generator Based on Boson Sampling:

Boson sampling is a restricted model of non-universal quantum computation. The model consists of sampling from the probability distribution of identical bosons scattered by a linear interferometer. In this research, Boson sampling is used to design a new quantum random number generator (QRNG) by effectively exploiting the randomness of the results of the Boson sampling. Its prototype system is built with a programmable silicon photonic processor, which can generate uniform and unbiased random sequences and overcome the drawbacks of the discrete QRNGs currently in use. Boson sampling is implemented as a random entropy source, and random bit strings with satisfactory randomness and uniformity can be obtained after post-processing the sampling results. As shown in Figure 1, in the boson sampling problem, the Fock state is input a passive linear optical interferometer and the output distribution is sampled with photon detectors.

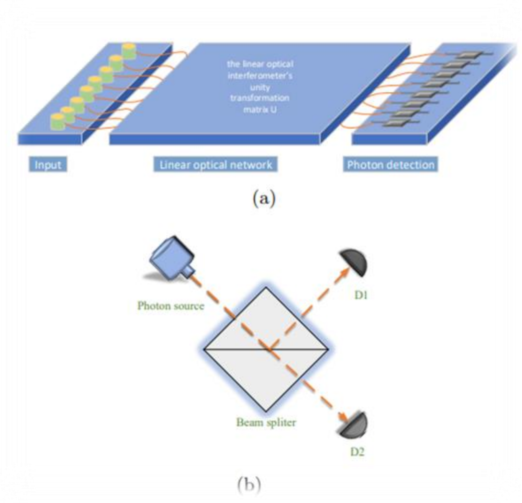


Figure 1: (a) n photons m modes Boson sampling model. n Bosons are input into the passive linear network of m modes, which is composed of beam splitters and phase shifters. After the interference effect of the network, the photons are detected and sampled by the detectors at the output modes. (b) The structure of Branching path QRNG. The photon is sent to a balanced beam splitter and the output is detected with the same probability.

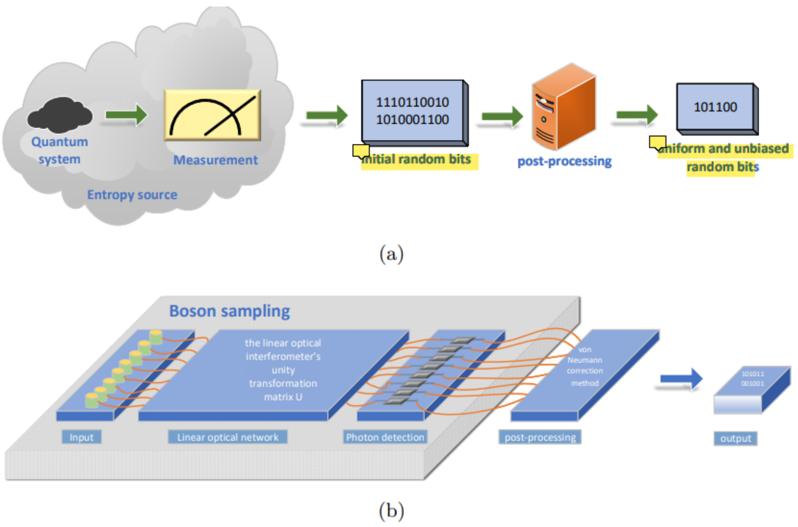
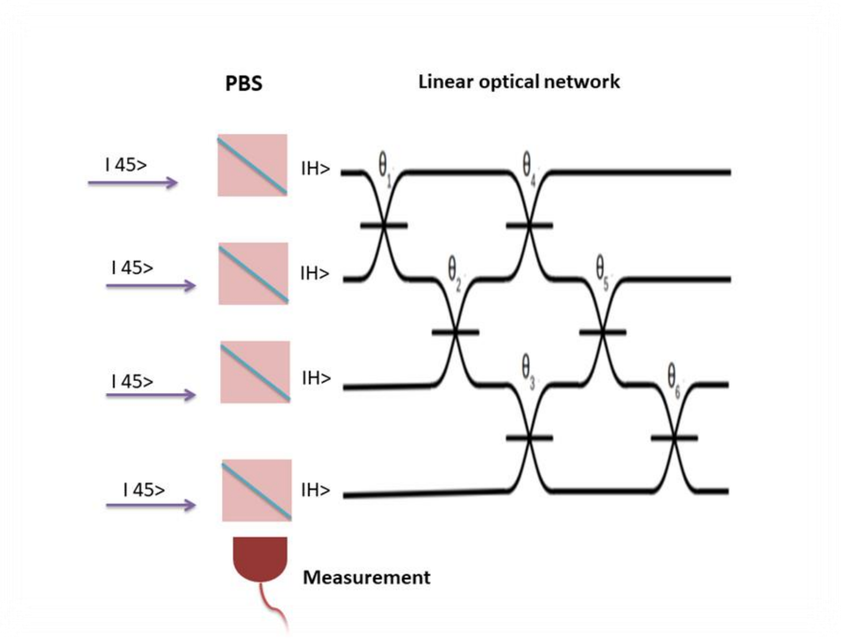


Figure 2: (a) Block structure of QRNG.(b) The structure of Boson sampling-based QRNG.

As shown in Figure 2, the block structure of QRNG consists of the entropy source and the post-processing. The entropy source includes the quantum system and the measurement process, generating the initial random numbers. The post-processing ensures the random number sequence can be uniform and unbiased with 0bit and 1bit derived on equal probability. (b) The structure of Boson sampling-based QRNG. The sampling results are post processed with Von Neumann correction method to obtain a uniform 01-bit sequence.

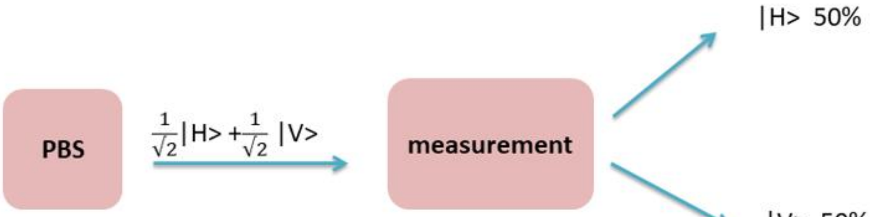
## Modified input state:

In the method mentioned in the previous section, they use the entropy source to generate random bits and finally, they generate uniform random bits with the post-processing method. The results show that there is a significant dissipation in this method. The number of loss states can be decreased and the speed of random number generation can be increased by changing the entropy source. We can use the intrinsic randomness property of quantum physics twice during the generation of random numbers to increase the randomness of the output if we change the experiment so that the input states of the linear optical network are chosen randomly and we have no control over it.



Input source scheme

In this design, the input of each optical fiber is coupled with a Polarizing beam splitter (PBS) in such a way that only photons with vertical polarization enter the optical mode. Polarizing Beam splitters are Beam splitters designed to split light by polarization state rather than by wavelength or intensity. Therefore, if we use photons with 45 degree polarization, we observe superpositions of the vertical and horizontal states of light in the PBS output. The measurement causes the collapse of the photon state to one of the vertical or horizontal polarizations. If the measurement causes the photon's H polarization state to collapse, we therefore have photons on these photonic modes.



In this method, we use the intrinsic randomness property of quantum physics (measurement effect on superposition states) to prepare input states to the optical linear network. This causes us to have random input states for each system execution. In this method, the input states of the linear optical network are randomly selected, so we can generate the desired random bit sequence with just one sampling and recording the results, so The number of loss states can be decreased and the speed of random number generation can be increased.