Difference between true random numbers and pseudo random numbers

Tian Xiaoyang
26001904581

Pseudo random number generators are also known as deterministic random bit generator. It is an algorithm for generating a sequence of number whose nature is close to that of a random sequence. However, PRNG is not truly random because it is completely determined by an initial value called the seed. Even though the seed can be a truly random value, the sequence generated after seed is actually determined when the seed is generated.
Since it is not truly random, the sequence generated by PRNG will repeat itself eventually, making the pattern periodic.
The sequence can also be replicated at a later time if given the same seed.
PRNG are often in simulation and modeling applications, where its pseudo randomness would simulate true randomness, and its predictable periodic pattern would help set a model.

True random number generators, also known as hardware random number generator, can generate truly random sequence of numbers based on a physical process instead of an algorithm. They are often based on microscopic phenomena which generate low-level, statistically random noise signals. These processes are in theory completely unpredictable as long as there’s no computable/known equation governing the process.
Natural physical phenomena that can be used to generate random values include: dice, nuclear decay, or Shot noise, a quantum mechanical noise source in electronic circuits, etc.
A TRNG usually consists of a transducer to convert physical phenomena to electrical signal, and an amplifier to increase the magnitude of random fluctuations to measurable level.
TRNG are often used in cryptography. Due to its nearly true randomness and unpredictability, it is used to create random encryption keys. PRNG can also be used for cryptography, however due to its predictability, TRNG encryption still provides the greatest safety for data security.