Entropy-as-a-Service: A Post-Quantum Random Number Generator Using Johnson-Nyquist Noise for E-Gaming

---

Abstract
This project presents a hardware-based random number generator (HRNG) leveraging Johnson noise as a true entropy source. The system integrates a resistive noise source, ADC, and FPGA/microcontroller for real-time random number generation, enhanced through post-processing techniques like whitening. This can be used for generating True Random Number Generator for Entropy-as-a-Service (EaaS) for Online gaming platforms.

Problem Statement

Risk of Prediction in online gaming is one of the most challenging task to be dealt with when launching gambling games. The conventional method of generating Random numbers are prone to prediction because the currently used Software based algorithms such as Linear Congruential Generators produces Pseudo-Random Numbers. Popular Hardware Random Number Generators including from Intel have recently been reported as exploited. With the upcoming Quantum Computing Era, the risks will be heightened to its peak

Solution

For solving the problem we need a True random Number Generator and for that purpose, we propose a Hardware random Number Generator based on Johnson-Nyquist Thermal Noise as a source of Entropy. The entropy from this source will be extracted, amplified and will be processed for conversion to digital format and this true random number could be used for Online gaming services.

Block Diagram