Johnson-Nyquist Noise Based Multi-Purpose Hardware Random Number Generator

Guide: Prof. Jinu Jayachandran

MOHAMMED SUHAIL K M (TVE22AE040)
MUHAMMED MIDLAJ M P (TVE22AE041)
SREYAS KISHORE T (TVE22AE062)
VAISHNAV U (TVE22AE064)

Department of Electronics and Communication Engineering
College of Engineering Trivandrum

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. Applications include load balancing, CAPTCHA generation, OTP creation, IoT sleep-wake scheduling, random IP Address assignment, and Entropy-as-a-Service (EaaS) for secure cloud-based services. Combining high-quality randomness with scalability, this HRNG offers a robust, cost-effective solution for cybersecurity, IoT, and distributed computing applications.

Objective

To design and implement a hardware random number generator (HRNG) leveraging Johnson noise for generating true random numbers, integrated with FPGA or microcontroller platforms for applications such as load balancing, CAPTCHA and OTP generation, IoT sleep-wake scheduling, random IP address Assignment, and Entropy-as-a-Service (EaaS).

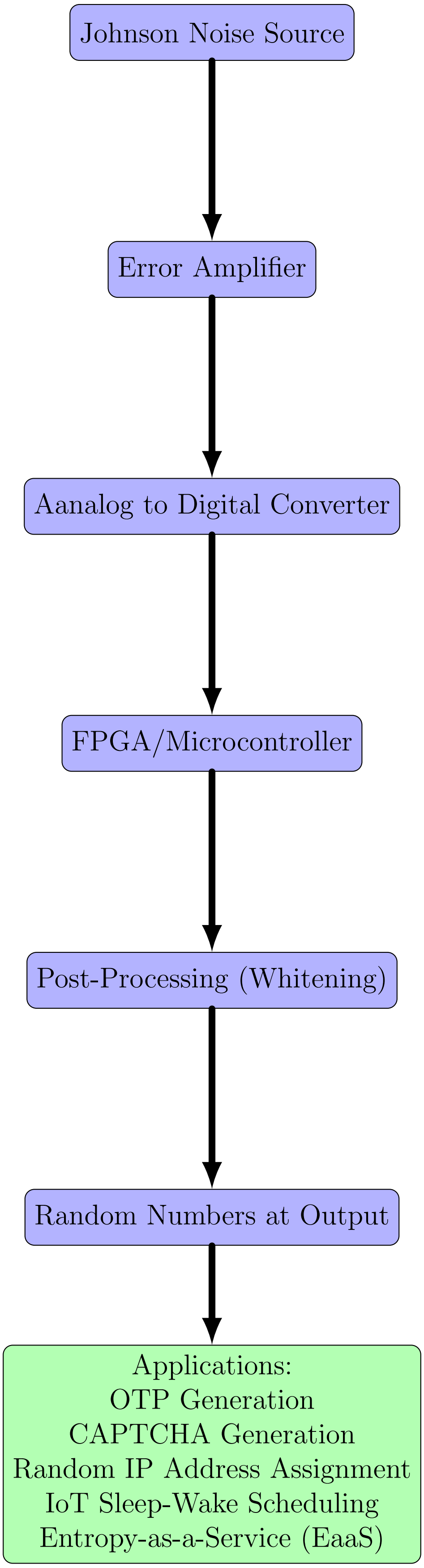
Motivation

Random number generation is essential in cryptography, cybersecurity, IoT, and cloud services. Existing methods often rely on pseudo-random algorithms, which lack true entropy and are vulnerable to prediction. Leveraging Johnson noise as a natural entropy source ensures high-quality randomness and enhances system security and reliability.

Impact

The proposed HRNG offers a reliable, scalable, and cost-effective solution for diverse applications, from secure communications and distributed systems to IoT Devices' energy management and Entropy-as-a-Service (EaaS). Its integration into modern platforms ensures widespread adoption, improving security and efficiency in critical systems.

Block Diagram


Johnson Noise Source
Error Amplifier
Aanalog to Digital Converter
FPGA/Microcontroller
Post-Processing (Whitening)
Random Numbers at Output
Applications:
OTP Generation
CAPTCHA Generation
Random IP Address Assignment
IoT Sleep-Wake Scheduling
Entropy-as-a-Service (EaaS)