Pseudo Random Number Generator

Vishwas Narendra Puniya
LMU Munich

June 22, 2025

Abstract

In this experiment, I build and analyze a Pseudo Random Number Generator (PRNG). I built the circuit using SN74HC175N D-type flip-flops and XOR gates.

1 AIM

To build a Pseudo Random Number Generator (PRNG) using digital logic components.

2 APPARATUS

- SN74HC175N D-type flip-flops
- XOR gates
- Breadboard
- Connecting wires
- Power supply
- PCB and Soddering tools
- Resitors
- LEDs

3 circuit diagram

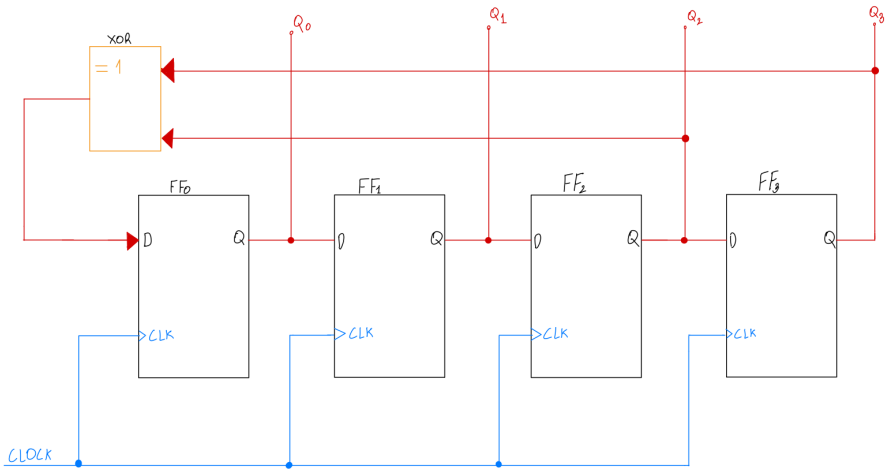

Figure 1: Circuit Diagram of the Pseudo Random Number Generator

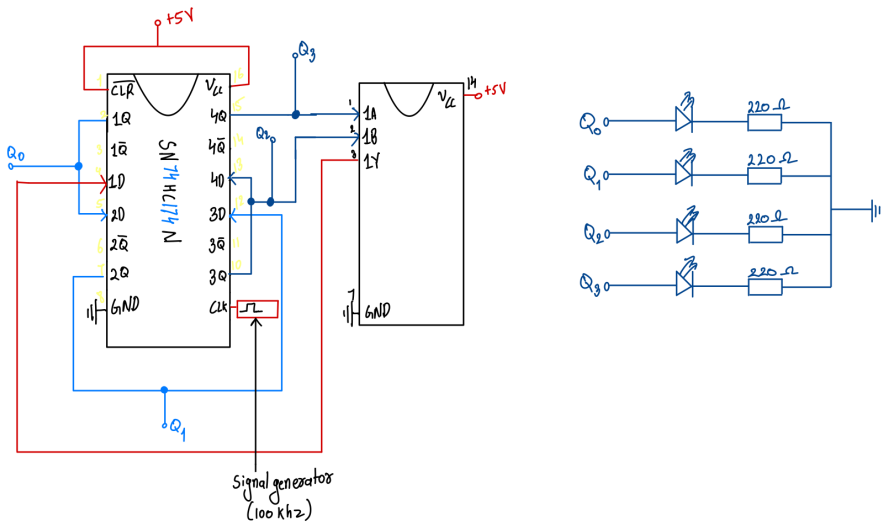

Figure 2: Circuit Diagram of the Pseudo Random Number Generator with Pinout

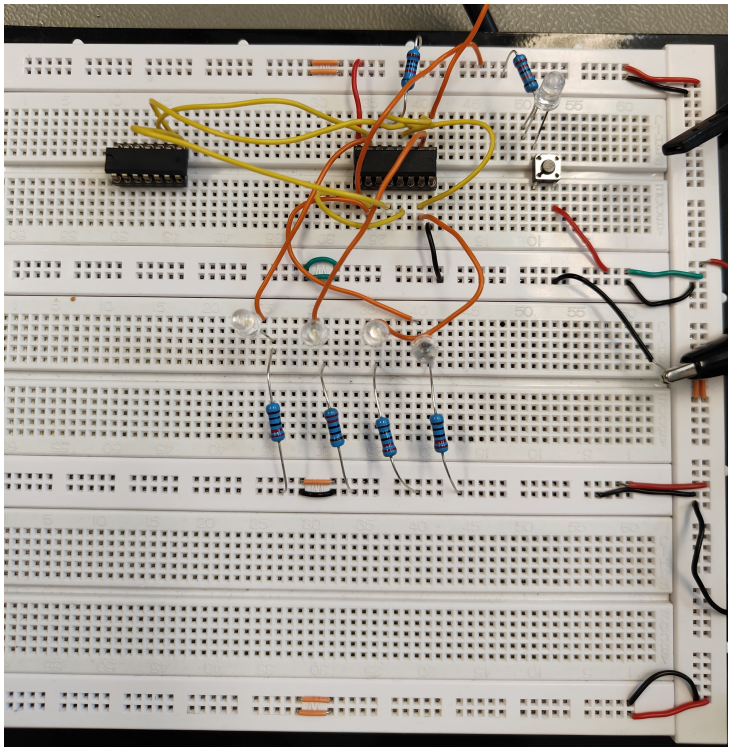

Figure 3: Circuit Diagram of the Pseudo Random Number Generator on the soderless breadboard

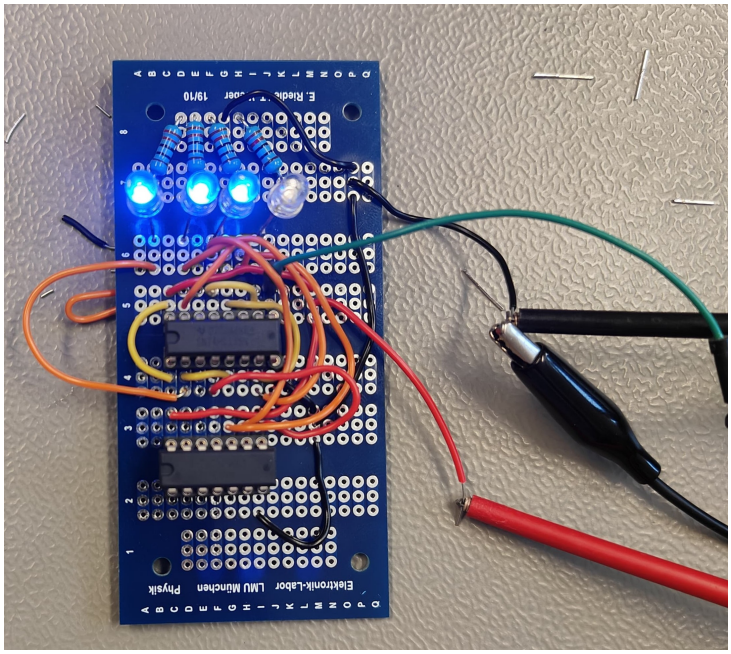

Figure 4: Circuit Diagram of the Pseudo Random Number Generator On PCB

4 Working

The circuit shown implements a 4-bit Linear Feedback Shift Register (LFSR), a type of sequential logic circuit used for generating pseudorandom sequences. It consists of:

- Four D-type flip-flops labeled FF_0 to FF_3, connected in series.
- A feedback loop implemented using a two-input XOR gate.
- A common clock signal driving all flip-flops synchronously.

Operation

At each rising edge of the clock:

1. The XOR gate computes the feedback bit as the exclusive-OR of the outputs Q_0 and Q_3 of the first and last flip-flops:

$$D_0 = Q_0 \oplus Q_3$$

2. The new input bit D_0 is fed into FF_0.
3. The current values of the flip-flops shift to the right:

$$Q_3 \leftarrow Q_2, \quad Q_2 \leftarrow Q_1, \quad Q_1 \leftarrow Q_0$$

4. The register output at any time is the combined state $[Q_3, Q_2, Q_1, Q_0]$.

Pseudo Random Number Generation

- The initial state must be non-zero to avoid the register locking into the zero state.
- The LFSR generates a pseudo random binary sequence with a maximal length of $2^4 - 1 = 15$ unique states before repeating, provided the feedback taps are chosen correctly.
- In this case, taps are from Q_0 and Q_3, which form a maximal-length LFSR.

5 RESULTS

The Pseudo Random Number Generator (PRNG) was successfully built and tested.