Lab - 4

8-bit Pseudo-Random Number Generator

Random Number Generator[1]

- A sequence of numbers or symbols generated
  - that cannot be reasonably predicted better than by random chance.
- Examples of Random Number generation?

Random Number Generator

- A sequence of numbers or symbols generated
  - that cannot be reasonably predicted better than by random chance.
- Examples of Random Number generation?
  - Dice
  - Coin Flip
  - Shuffling of Playing Cards, etc.

True Random Number Generation

- Generation is a function of the current value of a physical environment attribute
- Constantly changing
- Practically impossible to model !!

Pseudo-Random Number Generators[2]

- “Not truly Random”
- Generate numbers that only look random
- Are in fact predetermined
- Can be reproduced simply by knowing the state (initial state - seed)

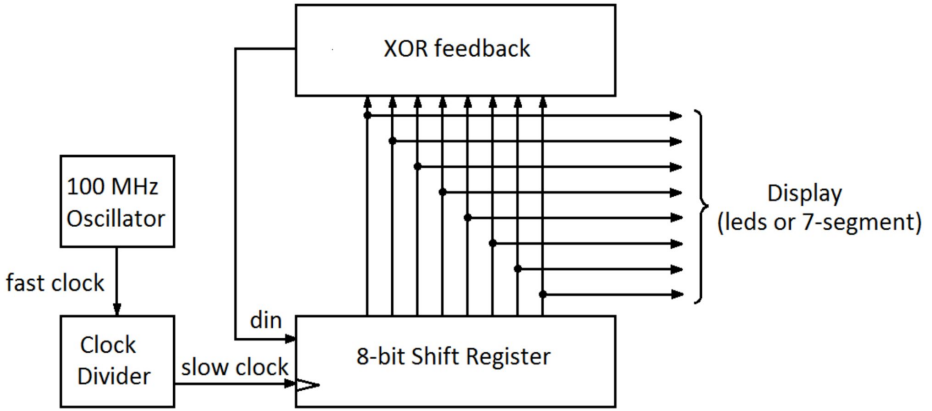
Think of a way, one can achieve close to true random number generator!!

Pseudo-Random Number Generators (cont.....)

- There are lots of different algorithms for PRNGs[3]
  - Middle-Square Method - 1946
  - Linear Congruential Generator (LCG) - 1951
  - Lagged Fibonacci Generator (LFG) - 1958
  - Linear-feedback shift register (LFSR) - 1965
  - Squares RNG - 2020

Linear Feedback Shift Register[4] (LFSR)

- As the name suggests, it is a **Shift Register**
- Its input bit is a **linear function** of its previous state.
- Most commonly used Linear Function is eXclusive OR (XOR)
- Register has a finite number of possible states (2^n -1)
  - must eventually enter a repeating cycle
- Has a lot of applications
  - Cryptography
  - Digital Broadcasting
  - Digital Communication
    - HDMI 2.0
    - PCI Express
    - USB 3.0
    - BLE



References

[1] Random number generation
[2] Pseudorandom number generator
[3] List of random number generators
[4] Linear-feedback shift register

END

Any Questions?