EE5811 FPGA Lab Final Project

Deep Diwani:EE16BTECH11006
Shaik Khalid Basha:EE16BTECH11035

IIT HYDERABAD

Introduction to Random Number Generator

A random number generator, generates a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance.

Types of random number number generator:

1) Hardware Random Number Generators (HRNG)
2) Pseudo-Random Number Generators (PRNG)

Hardware Random Number Generators

Device that generates random numbers from a physical process, rather than by means of an algorithm.
Eg. By measuring temperature / some radiations in medium.

Pseudo-Random Number Generators

Device which generates numbers which look random, but are actually determined by an initial value called the seed.

Pseudo random number generators

- Middle-Square method
- Linear Congruential method
- Linear feedback shift register
- Xorshift
- Cryptographic Pseudo Random Number

LCG Random Number

$$X_{n+1} = (aX_n + c)\%m \tag{1}$$

Where a, c, m are Parameters.
m decides range in which random number has to be generated.

Implementation

```
int* lcg(int n) {
        int* x = malloc(sizeof(int)*n);
        int m = (int) pow(2,31);
        int c = 12345;
        int a = 1103515245;
        int seed = time(NULL);

        for(int i=0;i<n;i++){
                x[i] = (a*seed+c)%m;
                seed = x[i];
        }
        return x;
}
```

Xorshift Random number generator

Generate the next number in their sequence by repeatedly taking the exclusive or of a number with a bit-shifted version of itself.

Implementation

```
uint64_t xor_shift_128_plus() {
        uint64_t x = state[0];
        uint64_t const y = state[1];
        state[0] = y;
        x = (x) ^ (x << 23);
        state[1] = x ^ y ^ (x >> 17) ^ (x >>26);
        return state[1] + y;
}
```

And last

Thank You