Benny Chen
12/08/2021
SEC 004L

CSE 2301 Lab 13

Theory

Pseudo-Random Binary Sequence or PRBS generator is a type of generator that creates a seemingly random sequence by shifting the series of inputs (WXYZ) to the right and replacing the MSB with the XOR of the X and Y values. A PRSB generator can be used to encrypt and decrypt data to be sent. Compared to OTP, PRBS would have a shorter encode and decoder key.

Deliverables

Register A	Output Register	PRBS	Encrypted bit
0001	0000	0001	0
X000	1000	0000	0
XX00	0100	0000	0
XXX0	0010	0000	0
XXXX	0001	0000	0

Register A	Output Register	PRBS	Encrypted bit
0001	0000	0011	1
X000	1000	1001	1
XX00	0100	0100	0
XXX0	0010	1010	0
XXXX	0001	1101	0

Current state	Next state	Encrypted bit
0001	0000	1
0010	1001	0
0011	1001	1
0100	1010	1
0101	1010	0
0110	0011	1
0111	0011	0
1000	0100	0
1001	0100	1
1010	1101	0
1011	1101	1
1100	1110	1
1101	1110	0
1110	0111	1
1111	0111	0

Discussion

This lab was actually very interesting as it looks somewhat like cryptography with encoding and decoding a set of data. This lab was daily easy to put together and understand and it was just shifting a number then flipping it twice.

Questions

If we add a 0000 state to our PRBS generator then it won't produce anything and would just output the input. When the clock is cycled, 0 XOR 0 is still 0 so nothing will change for the output. Instead of using a XOR to flip the bits, we can use a XNOR so the like values of 0 and 1 would produce 1. The shortcoming would be that it would be shifted differently with different bits but the end product would still be the same and would still be pseudo-random.