HW #2

Travis Collins
traviscollins@wpi.edu
ECE 578 Crytography and Data Security

September 23, 2012

1 Question 1: Linear Complexity

Note: All answers used Matlab code appended to end of homework.

a 0101010101

$$X = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} rank(X) = 2$$

Linear Complexity: m=3

b 011001100110

$$X = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} rank(X) = 3$$

Linear Complexity: m=4

c 011011011011011

$$X = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} rank(X) = 3$$

Linear Complexity: m=4

d 1011010010110

$$X = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} rank(X) = 5$$

Linear Complexity: m=6

Clock	*Initial*	1	2	3	4	5	6	7	8
$LFSR1$	1	0	1	1	0	1	1	0	1
$LFSR2$	1	0	0	0	0	1	1	1	1
$LFSR3$	1	1	0	0	0	0	0	0	0
Output	0	1	0	0	0	1	1	1	1

2 Question 2

A: Degree of stream generator

$$m = 3$$

B: Initialization Vector

$$S = [001]$$

C: Feedback Coefficients

$$F = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

3 Question 3

No this does not significantly improve over using single a LFSR. By XORing two LFSR's together we can at most double their complexity. For example if we take two LFSR of length 3, with coefficients

$$F1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} F2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

If they are XORed together, the linear complexity of their output at most is m=6, depending on input.

4 Question 4

b: Output

$$Output = [01001111]$$

c: Sequence length

Yes the condition of the length's being relatively prime is true, and the length of the output sequence is: