HomeAssignmentI

EE720

September 2020

Note: Total marks 20. Please submit the assignment file in PDF.

1. Figure 1 shows a scaled down version of the Trivium stream cipher. Write down the mathematical model of the cipher as a finite state dynamical system with output

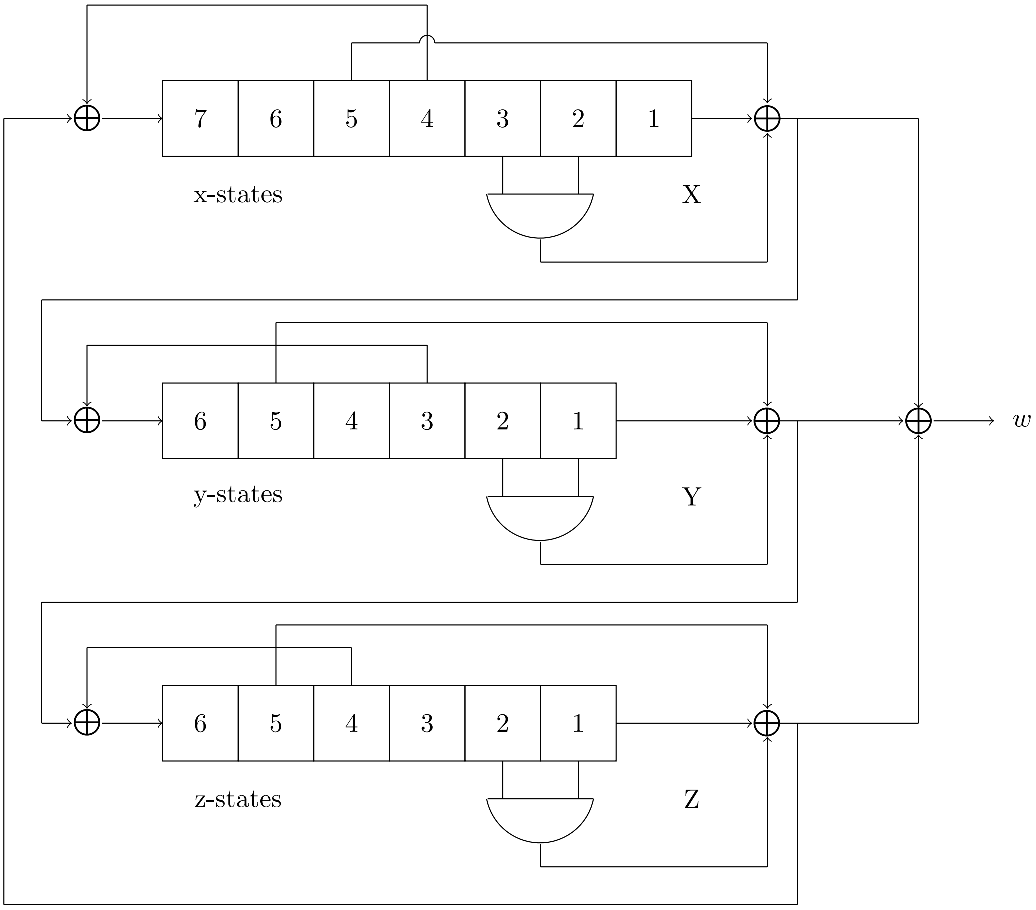
$$\begin{array}{lcl} x(k+1) & = & F(x(k)) \\ w(k) & = & f((x(k)) \end{array}$$

   where $x(k)$ denotes the state of the system which is the combined state of all registers X, Y, Z. The output of the cipher is denoted $w(k)$. Determine giving reasons whether the state update map is invertible. (5 marks).

2. Generate an output stream of 20 bits using the stream cipher of problem 1 from time index $k = 20$ to $k = 39$. Choose the initial loadings of the registers X, Y, Z from the bit stream obtained from a random 5 digit number by representing each digit in 4 bits and dropping the leftmost bit. For example if you choose the random number as 54794 then the bit stream of 20 bits for initial loading is (0101)(0100)(0111)(1001)(0100) by dropping the leftmost bit the registers are loaded as $X(0) = [1010100]$, $Y(0) = [011110]$, $Z(0) = [010100]$. (5 marks).

3. Find a primitive element of $\mathbb{F}_{2^6}$. Denote a root θ of the generating polynomial X^6+X+1 of the field and the field represented in basis $\{1, \theta, \ldots, \theta^5\}$. Find an element of order equal to largest prime divisor of order of $\mathbb{F}_{2^6}^*$. Find $(\theta^{5/2})$ in this field. Find order of $\theta + 1$. (5 marks).

4. Find roots of the quadratic equation $X^2 + (\theta)X + (\theta + 1) = 0$ in the field $\mathbb{F}_{2^6}$. Explain your method. Choose the representation of the field as in Problem 3. (5 marks).



	Register Length	**FB bit**	**FF bit**	**AND inputs**
X	7	4	5	2,3
Y	6	3	5	1,2
Z	6	4	5	2,3

Figure 1: Scaled down version of Trivium cipher