Class258 : Mathematical models of stream ciphers

Virendra Sule

August 25, 2020

1 Stream ciphers, PR generators

In the diagrams we saw two different classes of stream ciphers, non-linear combiners of outputs of lFSRs and combinations of irregularly clocked LFSRs. To simulate these stream ciphers or use them to generate PR sequences we need to consider the mathematical models and then implement the models in either hrdware or computer programs.

1. Mathematical model of an LFSR: Consider an LFSR $L[0,1,1,0]$. This is LFSR with register length of 4. The state at an instant k is $x(k) = (x_0(k), x_1(k), x_2(k), x_3(k))$. The recurrence rule is given by

$$x_4 = x_1 \oplus x_2$$

Then the state update model is

$$x(k+1) = (x_1(k), x_2(k), x_3(k), x_1(k) \oplus x_2(k))$$

Output at k is $w(k) = x_0(k)$.

2. Non-linear combination of $L1[0,1,1,1]$, $L2[1,0,1,0]$ and $L3[1,0,1]$: Consider states of the three LFSRs be denoted by vectors $x(k)$, $y(k)$, $z(k)$. Let the nonlinear combiner output be defined by

$$w(k) = w_1(k)w_2(k) \oplus w_1(k)w_3(k) \oplus w_2(k)w_3(k)$$

The state update equations are

$$\begin{array}{lcl} x(k+1) & = & (x_1(k), x_2(k), x_3(k), x_1(k) \oplus x_2(k) \oplus x_3(k)) \\ y(k+1) & = & (y_1(k), y_2(k), y_3(k), y_0(k) \oplus y_2(k)) \\ z(k+1) & = & (z_1(k), z_2(k), z_0(k) \oplus z_2(k)) \end{array}$$

The output equation in terms of states is

$$w(k) = x_0(k)y_0(k) \oplus x_0(k)z_0(k) \oplus y_0(k)z_0(k)$$

3. Alternating step generator: Let the three LFSRs be as in the above example with states $x(k), y(k), z(k)$ with outputs w_1, w_2, w_3 respectively. The update of state of $L1$ is governed by the equation of update of $x(k)$ in the above equations. The updates of states of $L2$ and $L3$ are defined by following equations

$$\begin{aligned} y(k+1) &= (w_1(k) \oplus 1)(y_1(k), y_2(k), y_3(k), y_0(k) \oplus y_2(k)) \\ &\quad \oplus w_1(k)(y_0(k), y_1(k), y_2(k), y_3(k)) \\ z(k+1) &= w_1(k)(z_1(k), z_2(k), z_0(k) \oplus z_2(k)) \\ &\quad w_1(k)(z_0(k), z_1(k), z_2(k)) \end{aligned}$$

where $w_1(k) = x_0(k)$. The ouput stream is defined by

$$w(k) = w_2(k) \oplus w_3(k) = y_0(k) \oplus z_0(k)$$

4. (Homework). Write the mathematical model of updates of states of the A5-I cipher with $L1, L2, L3$ as in the above examples. The distinguished bits given by $b_1(k) = x_2(k)$, $b_2(k) = y_1(k)$ and $b_3(k) = z_2(k)$. The output of the cipher is given by

$$w(k) = w_1(k) \oplus w_2(k) \oplus w_3(k)$$

write the output $w(k)$ in terms of the state variables of the three registers.

1.1 Key and IV descriptions

In the above examples of ciphers, there are several possible ways to incorporate the key symmetric key K and the IV bits as described below

1. For the nonlinear combiner key can be a initial contents of one of the registers or one register along with few bits of a second register. Rest of the initial bits of the registers can be taken as IV bits.

2. In the alternating step generator, the device is only used for PR sequence generator not as a stream cipher. Hence there is no key and no IV. The PR output stream is governed by random selelction of initial loadings of the three registers. With sufficiently large lengths and additional algebraic conditions on recurrence relations, the generator creates a reasonable PR sequences for One Time Pads when the initial conditions are changed.