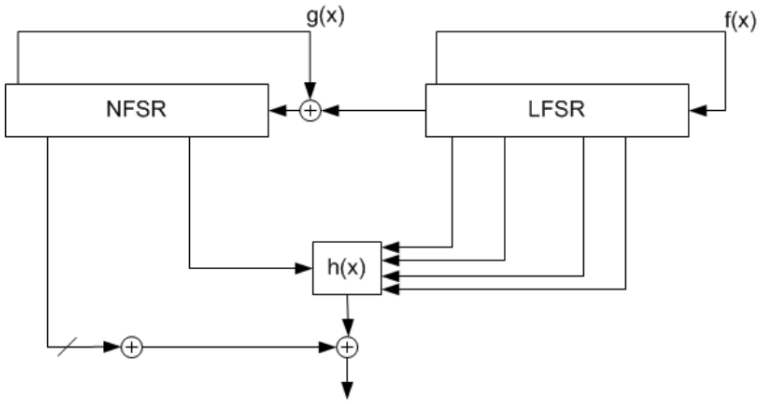
[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Akshay (202051018) — Lecture (Week 10)

1 Grain (A Stream Cipher) .... cont'd



1. It is based on one NFSR (80-bit), one LFSR (80-bit) and one non-linear filter function (h(x))
2. f(x) is feedback function of LFSR

   $s_{i+80} = s_{i+62} + s_{i+51} + s_{i+38} + s_{i+23} + s_{i+13} + s_i$

   $f(x) = 1 + x^{18} + x^{29} + x^{42} + x^{57} + x^{67} + x^{80}$ (primitive polynomial)

   Period $= 2^{80} - 1$
3. State bits are denoted by b_i and s_i in NFSR ans LFSR respectively
4. bit outputed by LFSR is xored with out of non-linear function g(x) and fed into NFSR as feedback bit

   $$\begin{aligned} b_{i+80} =& s_i + b_{i+62} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} + b_{i+21} + \\ &+ b_{i+14} + b_{i+9} + b_i + b_{i+63}b_{i+60} + b_{i+37}b_{i+33} + b_{i+15}b_{i+9} + \\ &+ b_{i+60}b_{i+52}b_{i+45} + b_{i+33}b_{i+28}b_{i+21} + b_{i+63}b_{i+45}b_{i+28}b_{i+9} + \\ &+ b_{i+60}b_{i+52}b_{i+37}b_{i+33} + b_{i+63}b_{i+60}b_{i+21}b_{i+15} + \\ &+ b_{i+63}b_{i+60}b_{i+52}b_{i+45}b_{i+37} + b_{i+33}b_{i+28}b_{i+21}b_{i+15}b_{i+9} + \\ &+ b_{i+52}b_{i+45}b_{i+37}b_{i+33}b_{i+28}b_{i+21} \end{aligned}$$
5. $h(x) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$

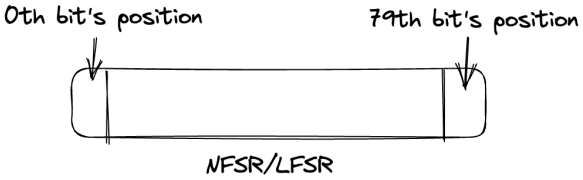
where the variables x_0, x_1, x_2, x_3 and x_4 correspond to the tap positions s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64} and b_{i+63} respectively. The output function is taken as

$$z_i = \sum_{k \in \mathcal{A}} b_{i+k} + h\left(s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64}, b_{i+63}\right)$$

where $\mathcal{A} = \{1, 2, 4, 10, 31, 43, 56\}$

1.1 Phase 1 - Key Initialization

We put 80 bit key in NFSR and 64 bit IV in LFSR.



Key, K = $(K_{79}, ..., K_0)$
$b_i = K_i$ (because key is placed in NFSR)
$IV = (iv_{63}....iv_0)$
Remaining 16 positions in LFSR are filled with 1. Because of this the LFSR cannot be initialized to the all zero state. Then the cipher is clocked 160 (=2*80) times without producing any running key.

2 RC4 Stream Cipher

R and C stands for the designers name. 4 stands for four lines of code.
We have to arrays of size N (= 256).
$S[i] = i \qquad$ for $0 \leq i \leq N-1$
$K = (K[0], ..., K[N-1])$
A secret key k of size l bytes.
$K[y] = k[y\%l] \qquad$ for $0 \leq y \leq N-1$

Initialisation:
for i = 0, ..., N-1 do
    S[i] = i
    j = 0
end

Scrambling:
for i = 0, ..., N-1 do
    j = (j - S[i] + K[i])
    Swap(S[i], S[j])
end

Output Generation:

Initialisation:
$i = j = 0$

Output Keystream Generation Loop:
$i = i + 1$
$j = j + S[i]$
Swap(S[i], S[j])
$t = S[i] + S[j]$
Output $z = S[t]$

3 Public Key Cryptography

Diffie - Helman key exchange algorithm.