LILI-II Stream Cipher

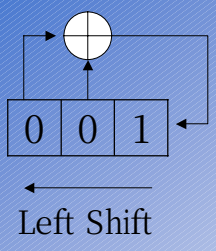
-- Hoonjae Lee(Dongseo Univ.)
-- Sangjae Moon(Kyungpook Nat' Univ.)
-- A. Clark (ISRC-QUT, Australia)
– E. Dawson (ISRC-QUT, Australia)
– J. Fuller (ISRC-QUT, Australia)
-- J. Golic (ISRC-QUT, Australia)
– W. Millan (ISRC-QUT, Australia)
– L. Simpson (ISRC-QUT, Australia)

Hoon-Jae Lee

hjlee@dongseo.ac.kr

http://cg.dongseo.ac.kr/~hjlee

LFSR(Linear Feedback Shift Register)



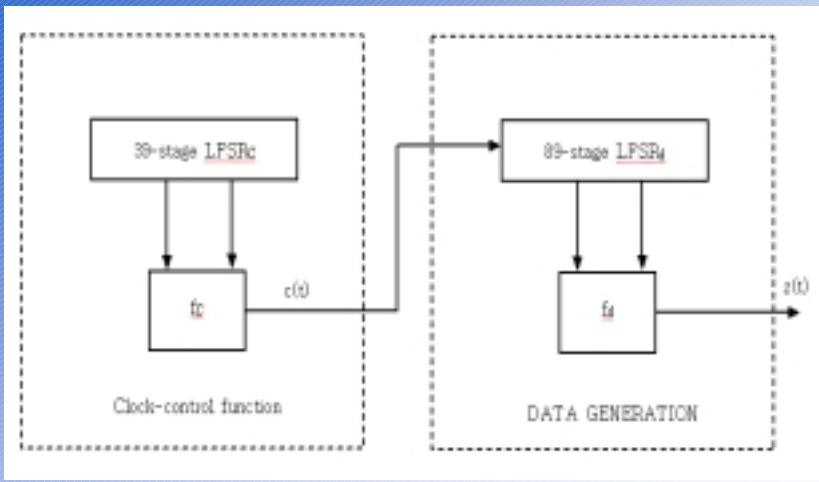
0 0 1 = (Initial state)
0 1 0 = (0 ⊕ 0)
1 0 1 = (0 ⊕ 1)
0 1 1 = (1 0)
1 1 1 = (0 1)
1 1 0 = (1 1)
1 0 0 = (1 1)
0 0 1 = (1 0)
0 1 0 = (0 0)
1 0 1 = (0 1)
0 1 1 = (1 0)
1 1 1 = (0 1)
1 1 0 = (1 1)
1 0 0 = (1 1)

Period = $2^3 - 1$
= 7

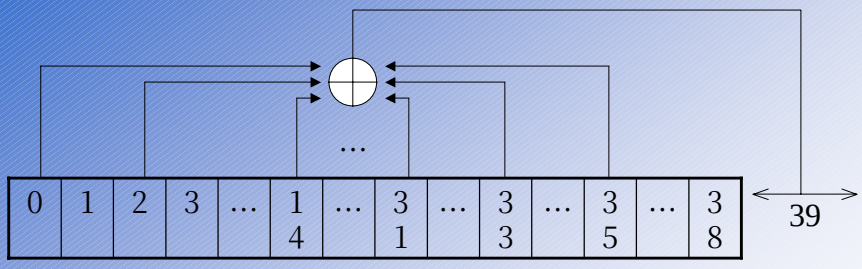
LILI-128 overviews

- LILI-128 Stream Cipher
  - NESSIE candidates, 2000
    (New European Schemes for Signature, Integrity, and Encryption)
  - QUT-ISRC, Australia, proposed
  - 128-bit key size (internal memory)
  - L. Simpson, E.Dawson, J.Golic and W. Millan
  - Attacked by Steve Babbage
  - Time-Memory Tradeoff Attack

LILI-128 Keystream Generator



39 -stage LFSRc



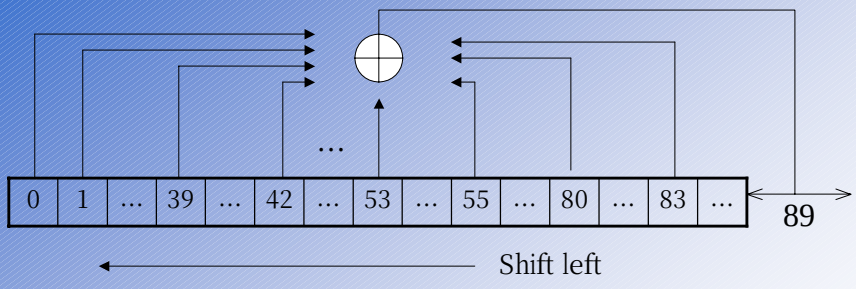
$$F(x) = x^{39} \oplus x^{35} \oplus x^{33} \oplus x^{31} \oplus x^{17} \oplus x^{15} \oplus x^{14} \oplus x^{2} \oplus 1 \Rightarrow 0$$
$$\Rightarrow x^{39} = x^{35} \oplus x^{33} \oplus x^{31} \oplus x^{17} \oplus x^{15} \oplus x^{14} \oplus x^{2} \oplus 1$$

Clock – Control Function (f_C)

- $f_C = 2*C_{12} + C_{20} + 1$

C_{12}	C_{20}	f_C	Clocks in $LFSR_d$
0	0	1	1
0	1	2	2
1	0	3	3
1	1	4	4

89 -stage $LFSR_d$



$$F(x) = x^{89} \oplus x^{83} \oplus x^{80} \oplus x^{55} \oplus x^{53} \oplus x^{42} \oplus x^{39} \oplus x \oplus 1 \Rightarrow 0$$
$$x^{89} = x^{83} \oplus x^{80} \oplus x^{55} \oplus x^{53} \oplus x^{42} \oplus x^{39} \oplus x \oplus 1$$

Data generation $f_d[1]$

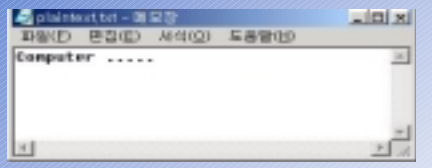
- f_d (0,1,3,7,12,20,30,44,65,80)

0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,
0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,
0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,
1,1,0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,0,0,1,1,1,1,1,0,0,1,1,0,0,0,0,0,1,1,
0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0,
0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0,
0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0,
1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,
0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0,0,1,1,0,1,0,1,1,0,0,1,1,0,
0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0,0,1,0,1,0,1,1,0,0,1,1,0,
0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,1,0,1,0,0,1,0,1,1,0,
0,1,1,0,0,1,1,0,0,1,0,1,1,0,0,1,1,0,0,1,1,0,1,0,1,0,0,1,1,0,
0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,
1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,
0,0,1,1,0,0,1,1,1,1,1,0,0,1,1,0,0,1,1,0,0,0,0,1,1,0,0,1,1,
1,1,0,0,1,1,0,0,0,0,1,1,0,0,1,1,0,0,1,1,1,1,1,0,0,1,1,0,0,
0,0,1,1,1,1,0,0,0,0,1,1,1,1,1,0,0,1,1,0,0,0,0,1,1,1,1,1,0,0,1,1,

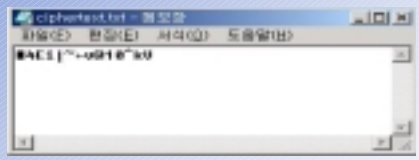
1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,
0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,
1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0,
0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,0,1,0,1,
1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,1,0,1,0,
0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,
1,0,1,0,0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0,
0,1,0,1,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1,
0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,
0,1,1,0,0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0,0,1,
1,0,0,1,1,0,0,1,0,1,1,0,0,1,1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0,
0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,1,0,1,0,0,1,1,0,0,1,
1,0,0,1,1,0,1,0,1,1,0,0,1,1,0,1,0,0,1,1,0,1,0,1,0,1,1,0,0,1,1,0,
0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,0,1,0,0,1,
1,0,0,1,0,1,1,0,1,0,0,1,1,0,1,0,0,1,0,1,1,0,1,0,1,0,1,1,0,1,0

LILI -128 Text Encryption

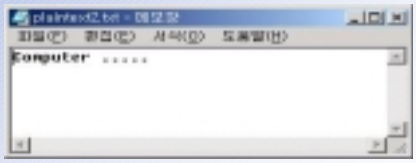
Plaintext →



Ciphertext →



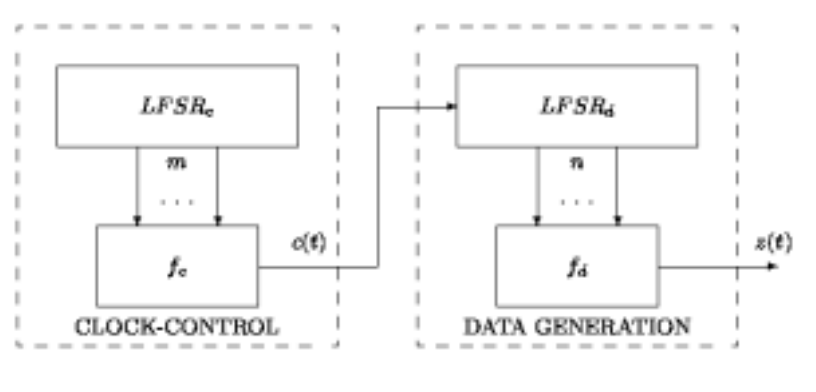
Rec.
Plaintext →



LILI -II overviews

- LILI -II Stream Cipher
  - ACISP'2002 proposed
  - Hoonjae Lee (Dongseo Univ.)
  - Sangjae Moon(Kyungpook Nat'l Univ.)
  - A. Clark, E.Dawson, J. Fuller, J.Golic, W. Millan and L. Simpson (QUT -ISRC, Austallia)
  - 255 -bit key size (internal memory)
  - Strong to Time -Memory Tradeoff Attack

LILI-II Keystream Generator



$LFSR_c$ and f_c

- Primitive Polynomial of $LFSR_c$

$$x^{128}+x^{126}+x^{125}+x^{124}+x^{123}+x^{122}+x^{119}+x^{117}+x^{115}+x^{111}+x^{108}$$
$$+x^{106}+x^{105}+x^{104}+x^{103}+x^{102}+x^{96}+x^{94}+x^{90}+x^{87}+x^{83}+x^{81}$$
$$+x^{80}+x^{79}+x^{77}+x^{74}+x^{73}+x^{72}+x^{71}+x^{70}+x^{67}+x^{66}+x^{65}+x^{61}$$
$$+x^{60}+x^{58}+x^{57}+x^{56}+x^{55}+x^{53}+x^{52}+x^{51}+x^{50}+x^{49}+x^{47}+x^{44}$$
$$+x^{43}+x^{40}+x^{39}+x^{36}+x^{35}+x^{30}+x^{29}+x^{25}+x^{23}+x^{18}+x^{17}+x^{16}$$
$$+x^{15}+x^{14}+x^{11}+x^{9}+x^{8}+x^{7}+x^{6}+x^{1}+1$$

- Clock-Controlled Function f_c

$$f_c(x_0, x_{126}) = 2(x_0) + x_{126} + 1.$$

$LFSR_d$ and f_d

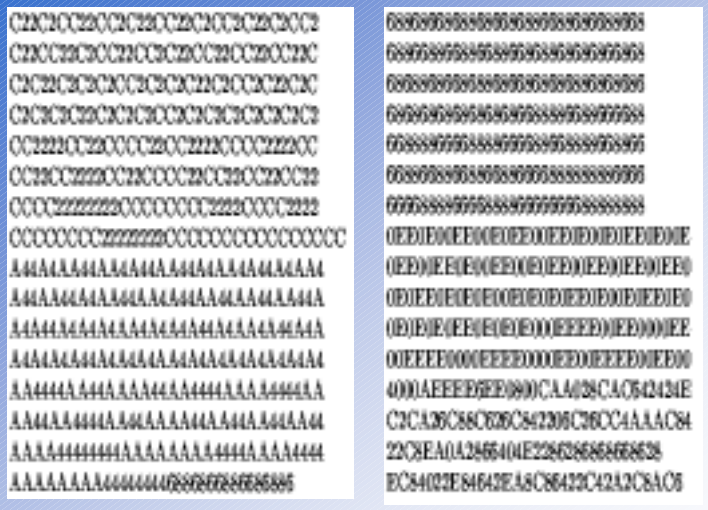
- Primitive Polynomial of $LFSR_d$

$$x^{127}+x^{121}+x^{120}+x^{114}+x^{107}+x^{106}+x^{103}+x^{101}+x^{97}+x^{96}+x^{94}$$
$$+x^{92}+x^{89}+x^{87}+x^{84}+x^{83}+x^{81}+x^{76}+x^{75}+x^{74}+x^{72}+x^{69}+x^{68}$$
$$+x^{65}+x^{64}+x^{62}+x^{59}+x^{57}+x^{56}+x^{54}+x^{52}+x^{50}+x^{48}+x^{46}+x^{45}$$
$$+x^{43}+x^{40}+x^{39}+x^{37}+x^{36}+x^{35}+x^{30}+x^{29}+x^{28}+x^{27}+x^{25}+x^{23}$$
$$+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{14}+x^{10}+x^{8}+x^{7}+x^{6}+x^{4}+x^{3}+x^{2}+x+1$$

- Data Generation Function f_d

$LFSR_d$ positions (0, 1, 3, 7, 12, 20, 30, 44, 65, 80, 96, 122)

$LFSR_d$ and f_d (2)

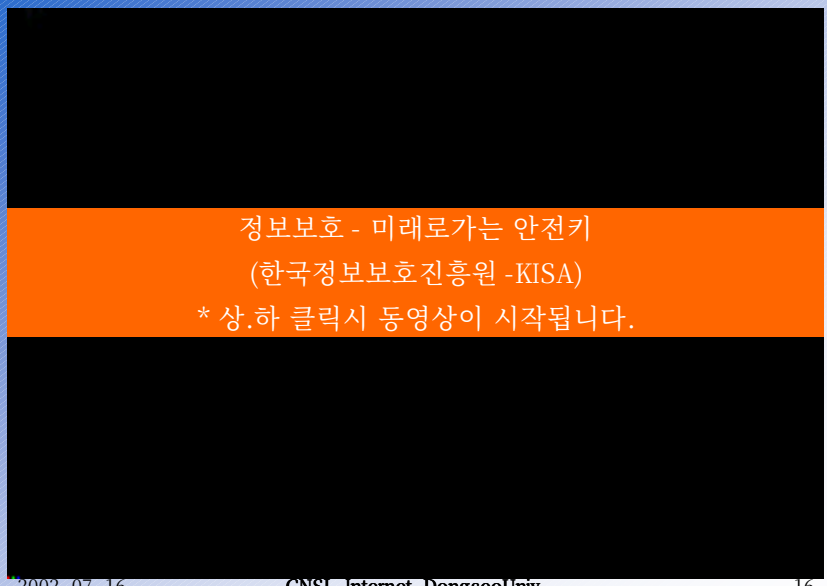
- 

$LFSR_d$ and f_d (3)

- Cryptographic Properties

The Boolean Function has 12 inputs and these properties:
Balanced, CI(1), Order=10, Nonlinearity=1992, No Linear Structures.

Digital Signature (Video)



정보보호 - 미래로가는 안전키
(한국정보보호진흥원 -KISA)
* 상.하 클릭시 동영상이 시작됩니다.


Break Time !
2002 -07 -16
CNSL -Internet -DongseoUniv.
17