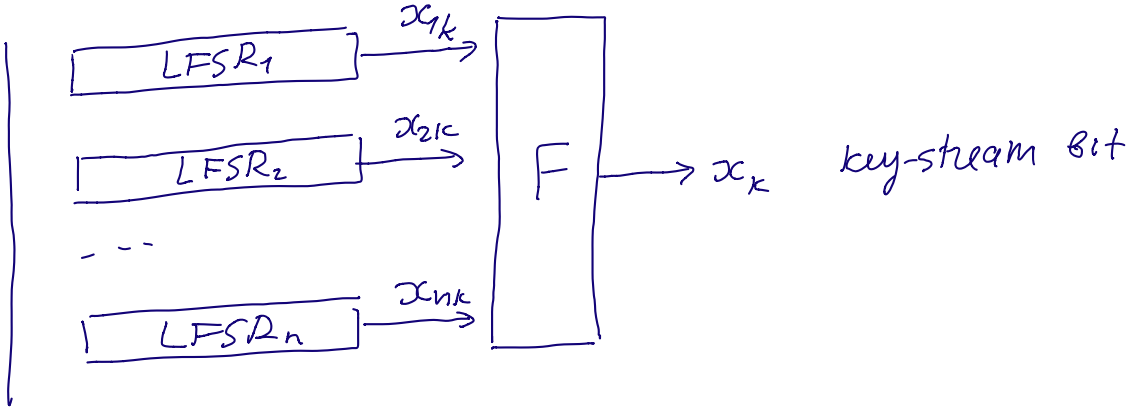
Combiners

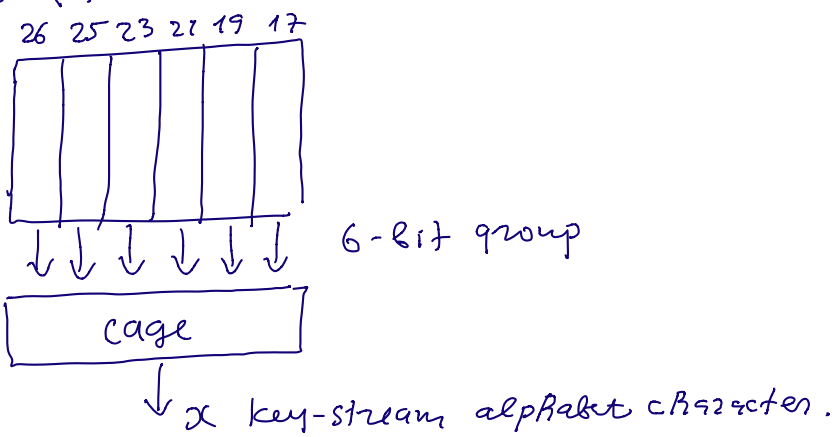
n LFSRs and a Boolean function

$$F = F(X_1, \dots, X_n)$$



$$x_k = F(x_{1k}\, x_{2k} \dots x_{nk})$$

Hagelin cipher (M-209)



Important characteristic of the key-stream is its min. period.

x_{ik} pure periodic of min. period T_i
(if LFSR$_i$ is used $\Rightarrow T_i = 2^{n_i} - 1$]
. prim. polynomial was used

x_k pure periodic of min. period t

We'll prove $t = T_1 \cdot T_2 \cdot \ldots \cdot T_n$ under some condition.

definition $F = F(X_1 X_2 \ldots X_n)$

X_1 is called relevant to F if there is a fixation $X_2 \ldots X_n = a_2 \ldots a_n$ s.t. $F(X_1 a_2 \ldots a_n) \neq$ constant.

(F really depends on X_1).

example. $F(X_1 X_2 X_3) = X_1 X_2$

X_1 is relevant $F(X_1, 1, 1) = X_1 \neq$ constant

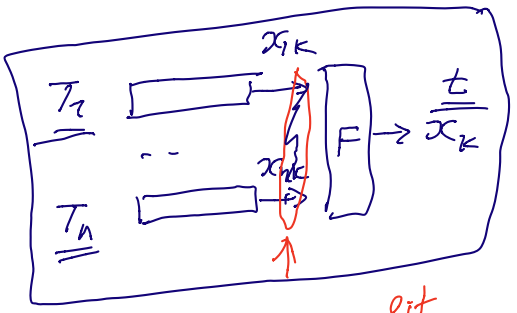
X_3 irrelevant $F(a_1 a_2 X_3) = a_1 a_2 =$ constant

Theorem. 1) $X_1, \ldots, X_n$ relevant to $F(X_1 \ldots X_n)$

2) $T_i > 1$

3) $\gcd(T_i, T_j) = 1 \quad i \neq j$.

Then $t = T_1 \cdot T_2 \cdot \ldots \cdot T_n$.



Lemma. $(x_{1k}\ x_{2k} \ldots x_{nk})$ $k = 1, 2, \ldots$ runs over all n-bit strings.

Proof of the Lemma.

By induction $n=1$ (x_{1k}) – any 1-bit string

since $T_1 > 1$

assume lemma correct for

$(x_{2k} \dots x_{nk})$

we'll prove the lemma

$X(k) = (x_{1k} x_{2k} \dots x_{nk})$

fix n-bit string $(a_1 a_2 \dots a_n)$

find k s.t. $X(k) = (a_1 a_2 \dots a_n)$

By induction

for some k

$(x_{2k} \dots x_{nk}) = (a_2 \dots a_n)$

denote $T' = T_2 \dots T_n$ and

$\gcd(T_1, T') = 1$.

$X(k+T's) = (x_{1k+T's}, x_{2k+T's} \dots x_{nk+T's})$

$s = 0, 1, \dots$ $= (x_{1k+T's}, x_{2k}, \dots, x_{nk}) =$

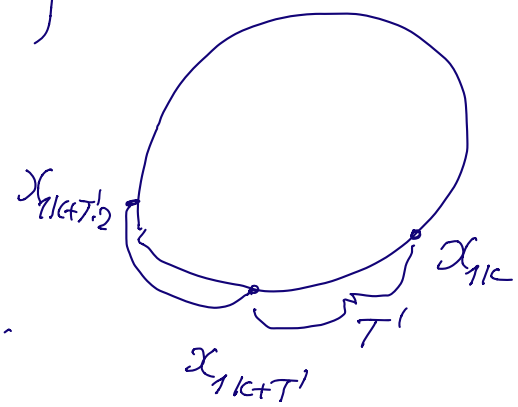
$= (x_{1k+T's}, a_2, \dots, a_n)$

min. period of $x_{1k+T's}$, $s = 0, 1, \dots$

is $T_1 > 1$ decimation of x_{1k} with

step T')

$\Rightarrow$ $x_{1\,k+T's}$ may have values 0 and 1.



there is s s.t.

$$x_{1\,k+T's} = a_1$$

$$\Rightarrow X(k+T's) = (a_1 a_2 \ldots a_n)$$ ▨

Proof of the Theorem.

1) We'll prove T_1 / t

X_1 relevant to $F(X_1 | X_2 \ldots X_n)$

find fixation $X_2 \ldots X_n = a_2 \ldots a_n$

s.t. $F(X_1, a_2, \ldots, a_n) \neq$ constant

$= X_1 + \beta$, β constant.

$\begin{matrix} 0 \\ 1 \end{matrix}$ $\left\{ \begin{matrix} X_1 \\ X_1 + 1 \end{matrix} \right.$

find k s.t. $(x_{2k} \ldots x_{nk}) = (a_2 \ldots a_n)$

$=$ by Lemma.

key-stream

t $\| x_{k+T's} = F(x_{1\,k+T's}, | x_{2\,k+T's}, \ldots, x_{n\,k+T's}) =$

$T' = T_2 \cdot \ldots \cdot T_n$

$= F(x_{1K+T's}, a_2, \ldots, a_n) =$

for any s

$= x_{1K+T's} + B_1$ T_1

min. period of $x_{1K+T's} + B$ is T_1

because decimation of $x_{1K}+B$ with step T' and $\gcd(T', T_1) = 1$.

period of $x_{K+T's}$ $s = 0, 1, \ldots$ is t

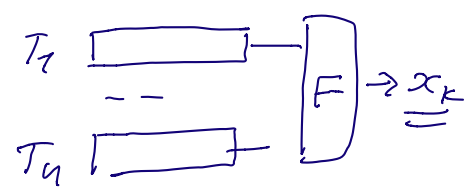
decimation of x_K $K = 0, 1, \ldots$

$T_1 \mid t$

$\Rightarrow T_i \mid t \Rightarrow T_1 \cdot T_2 \cdot \ldots \cdot T_n \mid t$

2) $t \mid T_1 \cdot T_2 \cdot \ldots \cdot T_n$

because $T_1 \cdot T_2 \cdot \ldots \cdot T_n$ is a period of the key-stream x_K



$\Rightarrow t = T_1 \cdot T_2 \cdot \ldots \cdot T_n$.

use LFSRs with primitive polynomials of degrees n_i, non-zero initial states

$$T_i = 2^{n_i} - 1$$

when $\gcd(2^{n_i}-1, 2^{n_j}-1) = 1 \quad i \neq j.$

Lemma. $\gcd(2^{n_1}-1, 2^{n_2}-1) = 2^{\gcd(n_1,n_2)} - 1.$

Proof. Apply Euclid Algorithm to (n_1, n_2)

$$\begin{cases} n_1 = a_1 \cdot n_2 + b_1 & 0 \le b_1 < n_2 \\ n_2 = a_2 \cdot b_1 + b_2 & 0 \le b_2 < b_1 \\ b_1 = a_3\, b_2 + b_3 & 0 \le b_3 < b_2 \\ \cdots \\ b_{s-2} = a_s\, b_{s-1} + b_s & b_s = 0 \end{cases}$$

$$\Rightarrow \gcd(n_1, n_2) = b_{s-1}.$$

We'll use $\boxed{\gcd(a, b) = \gcd(a \bmod b, b)}$

$$\gcd(2^{n_1}-1, 2^{n_2}-1) = \gcd(2^{a_1 \cdot n_2 + b_1} - 1, 2^{n_2} - 1) =$$

$$2^{n_2} \equiv 1 \bmod 2^{n_2} - 1 \Rightarrow 2^{a_1 \cdot n_2 + b_1} - 1 \equiv 2^{b_1} - 1 \bmod 2^{n_2} - 1$$

$= ab + b_2$

$$= \gcd(2^{n_2}-1, 2^{b_1}-1) = \gcd(2^{b_1}-1, 2^{b_2}-1) = \dots$$

By the same argument

$$= \dots = \gcd(2^{b_{s-1}}-1, 2^{b_s}-1) = \gcd(2^{b_{s-1}}-1, 0) =$$

$$= 2^{b_{s-1}} - 1 = 2^{\gcd(n_1, n_2)} - 1. \quad \blacksquare$$

$T_1 = 2^{n_1}-1$ — n_1 →

$T_n = 2^{n_n}-1$ — n_n →

→ F →

$\gcd(n_i, n_j) = 1$

$(2^{n_1}-1) \cdots (2^{n_n}-1)$

↑

min. period of the key-stream.

Linear complexity of the key-stream.

Theorem. x_{ik} of lin. compl. L_i ($LFSR_i$ $L_i = n_i$)

Then Lin. complexity of x_{ik} is

$$\leq F(L_1, L_2, \dots, L_n)$$

F integer polynomial produced from ANF of comb. function F after change $\oplus$ to $+$.

example. $F = x_1 x_2 \oplus x_3$ Boolean ANF

$+$

$x_1 x_2 + x_3$

Proof.

Fact two sequences

$$x = x_1 x_2 \ldots$$
$$y = y_1 y_2 \ldots$$

$$xy = x_1 y_1, x_2 y_2, \ldots$$
$$x \oplus y = x_1 \oplus y_1, x_2 \oplus y_2, \ldots$$

$$L(xy) \le L(x) \cdot L(y) \quad (*)$$

$$L(x \oplus y) \le L(x) + L(y) \quad (**)$$

↑ proved

key-stream $x_k = F(x_{1k} x_{2k} \ldots x_{nk})$ $k = 1, 2, \ldots$

ANF $F = X_{i_1} \cdot X_{i_2} \cdots X_{i_t} \oplus X_{j_1} \cdot X_{j_2} \cdots X_{j_s} \oplus \ldots$

$$\Rightarrow x_k = \underbrace{x_{i_1 k} x_{i_2 k} \ldots x_{i_t k}}_{(*)} \oplus \underbrace{x_{j_1 k} x_{j_2 k} \ldots x_{j_s k}}_{(*)} \oplus \ldots$$

lin. comp. $\le L_{i_1} L_{i_2} \ldots L_{i_t}$

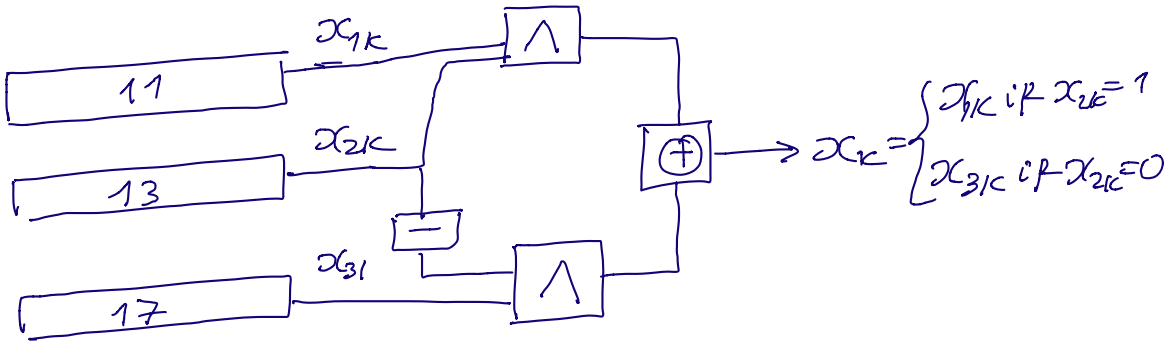
lin. comp. $\le L_{j_1} L_{j_2} \ldots L_{j_s}$

$$\Rightarrow L(x_k) \le L_{i_1} L_{i_2} \ldots L_{i_t} + L_{j_1} L_{j_2} \ldots L_{j_s} + \ldots$$

$$= F(L_1 L_2 \ldots L_n)$$

∎

Example. Geffer Generator



$$F = x_1 \cdot x_2 \oplus x_3 \cdot (x_2 \oplus 1) = x_1 \cdot x_2 \oplus x_2 x_3 \oplus x_3 = \begin{cases} x_1 & x_2 = 1 \\ x_3 & x_2 = 0 \end{cases}$$

period of x_k initial state of LFSRs = non-zero

$$T_1 = 2^{11} - 1, \quad T_2 = 2^{13} - 1, \quad T_3 = 2^{17} - 1.$$

$$\gcd(11,13) = \gcd(11,17) = \gcd(13,17) = 1.$$

$\Rightarrow$ min. period of x_k is

$$(2^{11}-1)(2^{13}-1)(2^{17}-1) \approx \underline{2.2 \cdot 10^{12}}.$$

lin. complexity

$$F = x_1 x_2 + x_2 x_3 + x_3$$

$$\text{lin. comp.}(x_k) \leq F(11,13,17) =$$

$$= 11 \cdot 13 + 13 \cdot 17 + 17 = 381.$$

lin. compl. $= \underline{381}$ possible to prove.