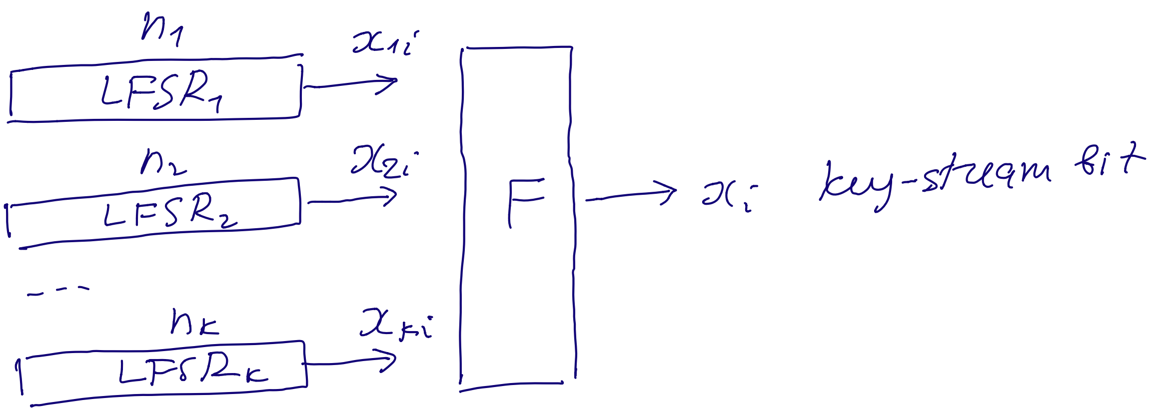
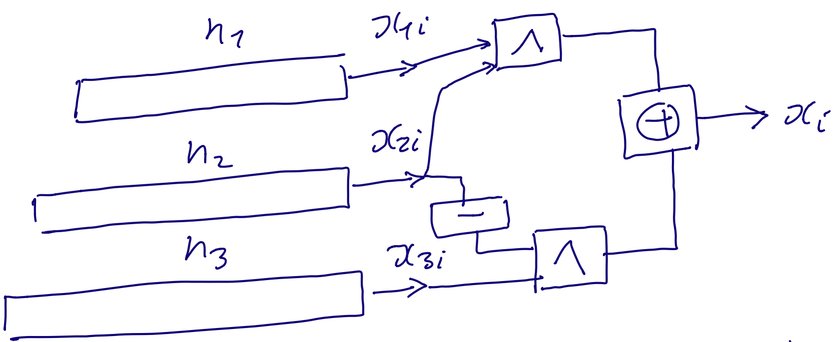
Correlation Attack for Combiners



task given $x^N = x_0 x_1 \dots x_{N-1}$

recover LFSRs initial states.

Geffe generator



Boolean function $F(x_1 x_2 x_3) = x_1 x_2 + x_3(x_2+1)$

correlation attack

1) find correlations between x_i, x_{1i}, x_{2i}, x_{3i}

2) Find LFSRs initial states separately.

brute force $2^{n_1+n_2+n_3}$

$$Pr\big(F(X_1X_2X_3) = X_1\big) =$$

$$= Pr(F = X_1, X_2 = 0) + Pr(F = X_1, X_2 = 1) =$$

complete probability formula

$$= Pr(X_3 = X_1, X_2 = 0) + Pr(X_1 = X_1, X_2 = 1)$$

$F(X_1\, 0\, X_3) = X_3$ and $F(X_1\, 1\, X_3) = X_1$

$$= \underbrace{Pr(X_2=0)}_{=\frac{1}{2}} \cdot \underbrace{Pr(X_3 = X_1)}_{=\frac{1}{2}} + \underbrace{Pr(X_2=1)}_{=\frac{1}{2}} \cdot \underbrace{Pr(X_1 = X_1)}_{=1}$$

$$= \frac{1}{4} + \frac{1}{2} = \frac{3}{4}.$$

Apply WH transform instead

x_1	x_2	x_3	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$$\begin{array}{r|cccccccc}
 & & v\,001 & & v & v & & v & \\
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\hline
 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
 & (0 & 2) & (2 & 0) & (0 & 2) & (-2 & 0) \\
 & (2 & 2 & -2 & 2) & (-2 & 2 & 2 & 2) \\
 & (0 & 4 & 0 & 4 & 4 & 0 & -4 & 0) \\
\hline
\text{WH spectrum} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & -\frac{1}{2} & 0
\end{array}$$

$$\Rightarrow \left[\begin{array}{l}
Pr(F = x_3) = \dfrac{1+\frac{1}{2}}{2} = \dfrac{3}{4} \\
Pr(F = x_2 + x_3) = \dfrac{1+\frac{1}{2}}{2} = \dfrac{3}{4} \\
Pr(F = x_1) = \dfrac{3}{4} \\
\hline
Pr(F = x_1 + x_2) = \dfrac{1-\frac{1}{2}}{2} = \dfrac{1}{4}
\end{array}\right.$$

all $0, x_2, x_1 + x_3, x_1 + x_2 + x_3$ prob. is $\frac{1}{2}$

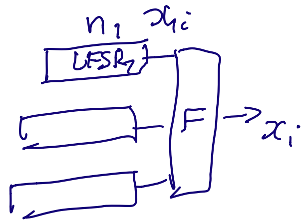
not usefull.

$Pr(x_i = x_{1i}) = \frac{3}{4} \Rightarrow x_i, x_{1i}$ correlated

$Pr(x_i = x_{2i}) = \frac{1}{2} \Rightarrow x_i, x_{2i}$ not correlated

---

How to find initial state of $LFSR_1$ in Geffe generator.



1. guess (try) all non-zero initial states of $LFSR_1$ ($2^{n_1} - 1$ possibilities)

2. generate $LFSR_1$ output sequence $\underline{\underline{x_{1i}'}}$ $i = 0, \dots, N-1$.

two cases

1) guess correct

$Pr(x_{1i} = x_i)$ $\|$

$\boxed{x_{1i}' = x_{1i}} \Rightarrow \boxed{Pr(x_{1i}' = x_i) = \frac{3}{4}}$

2) guess incorrect

$\Rightarrow \underline{x_{1i}' \neq x_{1i} \text{ in general}}$

can assume $\boxed{Pr(x_{1i}' = x_i) = \frac{1}{2}}$.

3. distinguish correct and incorrect guesses

compute $v_i = \underset{LFSR_1}{\underline{\underline{x_{1i}'}}} + \underset{\text{key-stream}}{\underline{\underline{x_i}}}$, $i = 0, 1, \dots, N-1$

guess correct $P_2(v_i = 1) = \frac{1}{4} = P_2(x'_{1i} \neq x_i)$

incorrect $P_2(v_i = 1) = \frac{1}{2}$

count N_1 # 1 in $v_0 v_1 \dots v_{N-1}$

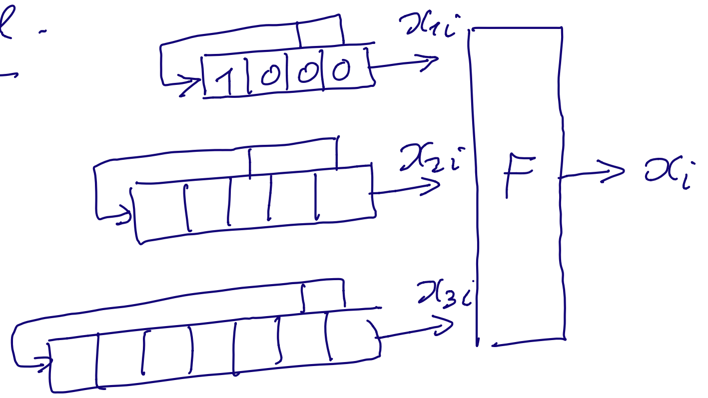
$\frac{N_1}{N} \to \frac{1}{4} \Rightarrow$ guess is correct

$\frac{1}{2}$ incorrect.

By Law of Large Numbers

dist. correct / incorrect if N is large enough.

Example.



x^4+x+1

x^5+x^2+1

x^7+x+1

$F = x_1x_2 + x_3(x_2+1) \Rightarrow$ Geffe generator.

$x = x^{20} = 11001 \mid 11100 \mid 01001 \mid 10101$

find $LFSR_1$ initial state. S_1

---

start guessing $S_1 = 1000$

$x' = 00010 \mid 01101 \mid 01111 \mid 00010$

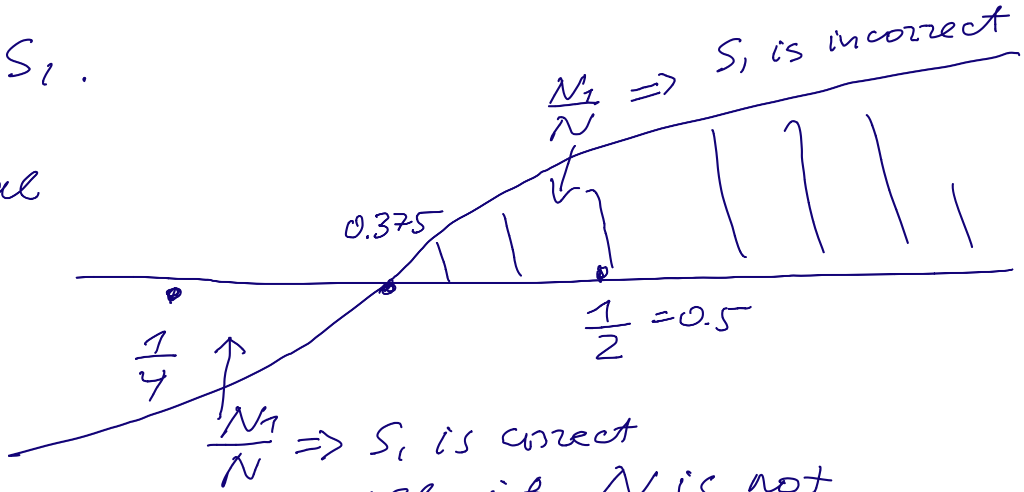
compute

$v = x + x' = 11011 \mid 10001 \mid 00110 \mid 10111$

$N_1 = 12$ $\qquad \dfrac{N_1}{N=20} = \dfrac{12}{20} = 0.6$ close to $0.5 = \frac{1}{2}$

reject S_1.

in general



some errors are possible if N is not large enough.

S_1	N_1/N, $N=10$		N_1/N, $N=20$	
1000	0.6		0.6	
...				
1100	0.8		0.65	
...				
0010	$\boxed{0.3}$	accepted	$\boxed{0.45}$	rejected
1001	$\boxed{0.3}$		$\boxed{0.45}$	
0101	$\boxed{0.2}$		$\boxed{0.1}$	accepted.
1011	$\boxed{0.3}$		$\boxed{0.5}$	rejected

for $\underline{\underline{N=10}}$ we have 4 candidate solutions.

$\underline{\underline{N=20}}$ we have 1 candidate solution.

Attack is effective if N is large enough.