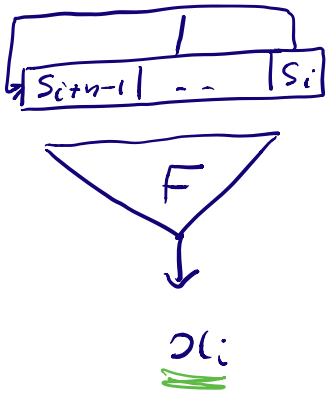
Fast Correlation Attack

1. Formula to compute a posteriori probabilities P_k.

2. How to solve systems of linear equations ? (modulo 2)



$$f(x) = x^n + x^{k_1} + \dots + x^{k_{t-1}} + 1$$

$k_t = 0 \qquad x^{k_t} = 1$

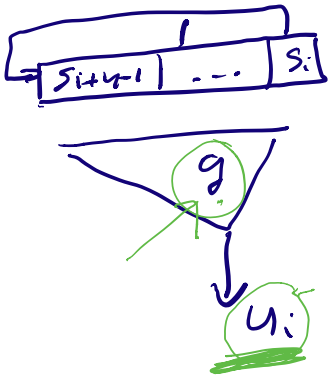
LFSR taps is t

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

find initial state $s_{n-1} \dots s_1 s_0$

g linear Boolean f.

with $p = P_2(F = g)$



$$p = P_2(z_i = u_i) = P_2(v_i = 0)$$

new variables

eliminate u_i

$$(*) \quad \begin{cases} v_i = u_i + z_i \\ i = 0, \dots, N-1. \end{cases}$$

use sparse relations $f(x)$ sparse feedback polynomial

$t+1$ = # non-zero terms in $f(x)$.

$f(x) = x^{41} + x^3 + 1$

$f(x) \rightarrow \begin{cases} u_{i+n} + u_{i+k_1} + \dots + u_{i+k_t} = 0 \end{cases}$

$f(x) \rightarrow \{ u_{i+2n} + u_{i+2k_1} + \dots + u_{i+2k_t} = 0$

combine (*) according to the sparse relations :

(**)

$$\begin{cases} v_{i+n} + v_{i+k_1} + \dots + v_{i+k_t} = x_{i+n} + x_{i+k_1} + \dots + x_{i+k_t} \\ v_{i+2n} + \dots = x_{i+2n} + \dots \end{cases}$$

check that all indices are in $\{0, \dots, N-1\}$

for every $0 \le k \le N-1$

find all relations (**) where v_k occurs

(***)

$$\begin{cases} v_k + v_{0_1} + \dots + v_{i_t} = R_1 \\ \dots \\ v_k + v_{j_1} + \dots + v_{j_t} = R_m \end{cases}$$

lin. comb. of the key-stream bits.

v_k occurs m times in (**)

compute a posteriori probability

$$P_k = P_r(v_k = 0 / (***))$$

1) $V = v_{i_1} + \dots + v_{i_t}$

$s = s(P, t) = P_r(V = 0) =$

$$= \underbrace{P_2(v_{i_1}=0)}_{P} \cdot \underbrace{P_2(v_{i_2}+\dots+v_{i_t}=0)}_{s(P,t-1)} +$$

$$+ \underbrace{P_2(v_{i_1}=1)}_{1-P} \cdot P_2(v_{i_2}+\dots+v_t=1) = 1-s(P,t-1)$$

(P agrees; 1-P)

complete probability formula

$$= P\cdot s(P,t-1) + (1-P)(1-s(P,t-1))$$

if take $t=1$

$$s = s(P,1) = P = P_2(v_{i_1}=0)$$

2) write (***) as

$$\begin{cases} v_k + V_1 = R_1 \\ v_k + V_m = R_m \end{cases}$$

v_k: 0 or 1; $V_1,\dots,V_m$: distinct, is known; $R_1,\dots,R_m$: known; $R_1,\dots,R_R$: 0; $R_{R+1},\dots,R_m$: 1 ($m-R$)

$$P_k = P_2(v_k=0/\dots) =$$

We know that exactly R of $R_1,\dots,R_m$ are 0.

event $A = \{R_1=\dots=R_R=0, R_{R+1}=\dots=R_m=1\}$

$$P_k = P_2(v_k=0/A) = \frac{P_2(v_k=0,\ A)}{P_2(A)} =$$

conditional probability formula

$$= \frac{P_2(v_k=0)\cdot P_2(A/v_k=0)}{P_2(A)}$$

$$P_2(A) = \underbrace{P_2(v_k=0)}_{p}\cdot P_2(A/v_k=0) + \underbrace{P_2(v_k=1)}_{1-p}\cdot P_2(A/v_k=1)$$

complete probability formula.

$$P_2(A/v_k=0) = P_2(V_1=\dots=V_R=0,\ V_{R+1}=\dots=V_m=1)$$

(independent)

$$= s^R\cdot(1-s)^{m-R}$$

same way

$$P_2(A/v_k=1) = P_2(V_1=\dots=V_R=1,\ V_{R+1}=\dots=V_m=0)$$

$$= (1-s)^R\cdot s^{m-R}$$

$$\Rightarrow P_k = \frac{p\cdot s^R\cdot(1-s)^{m-R}}{p\cdot s^R(1-s)^{m-R}+(1-p)(1-s)^R\cdot s^{m-R}}$$

done.

Algorithm to solve a system of linear equations.

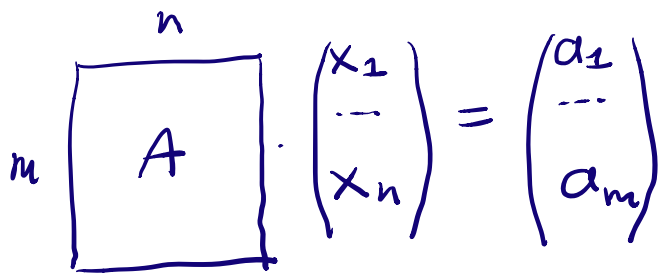
A $m \times n$ -matrix with entries $0, 1$.

a column m-vector

$x = (x_1 \dots x_n)$ column n-vector of unknowns

Problem: solve (find all solutions) to

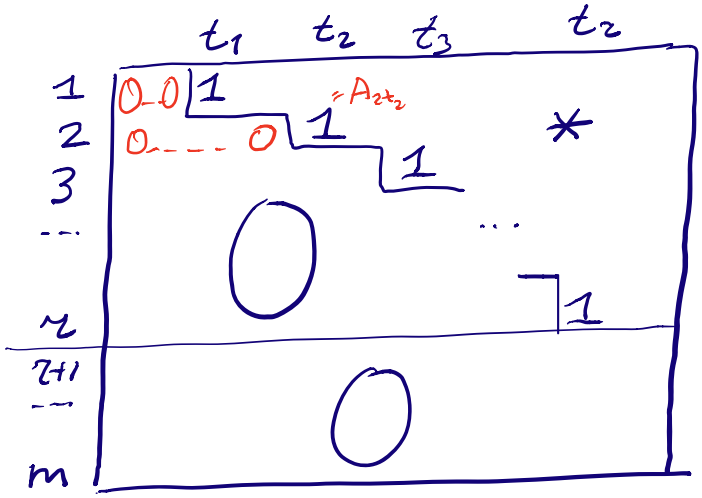
$$A \cdot X = a$$



notation A_i i-th row of A

A_{ij} (i,j)-entry of A.

definition A is in a row echelon form if:



e.g.

1	0	1	1	1
0	1	1	1	1
0	0	0	1	1
0	0	0	0	0

$r = \text{rank}(A)$. formally

there are numbers $0 \le r \le n$

and $0 = t_0 < t_1 < t_2 < \dots < t_r < t_{r+1} = n+1$

formally introduced.

s.t. 1) $1 \le i \le r$

$A_{ij} = 0 \quad 1 \le j < t_i$

$A_{it_i} = 1$

2) $A_{ij} = 0 \quad r+1 \le i \le m$

$1 \le j \le n$

Solving Algorithm

1. Augment A with column a and get

$M = A, a$

$m \times (n+1)$ - matrix

2. Reduce M to a row echelon form in first n columns

2.1 initialize $r = 0, \; t_r = 0$

2.2. nested loops

For j from $t_r + 1$ to n do

For i from $r+1$ to m do

(a) if $M_{ij} = 1$, then

$M_{r+1} \leftrightarrow M_i$ (row exchange)

For u from $r+2$ to m do

$M_u \leftarrow M_u + M_{uj} \cdot M_{r+1}$

break i and j-loop, go to 2.3

(b) if $M_{ij} = 0$, then continue

(c) if $M_{ij} = 0$ $t_{r+1} \leq j \leq n$

$r+1 \leq i \leq m$

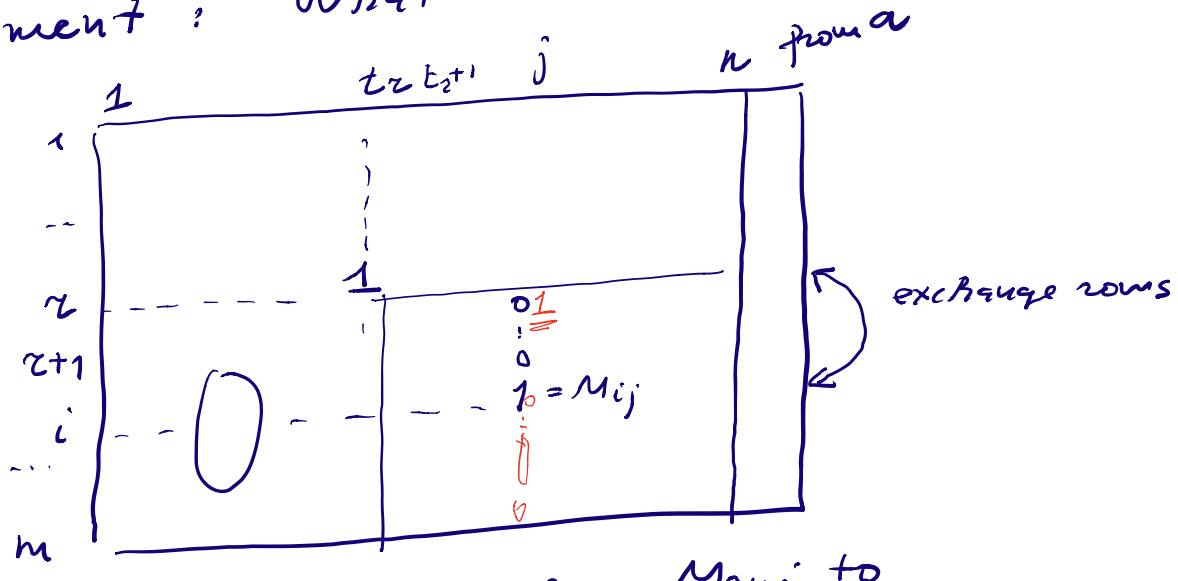
then terminate 2.

2.3 if $r = n$, then terminate 2

else $r \leftarrow r+1$ and $t_r \leftarrow j$

repeat 2.2.

comment: What 2.2 does?

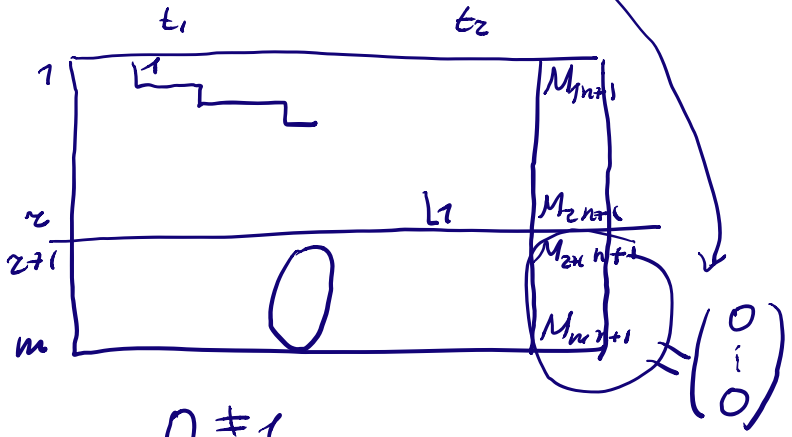


reduce all entries below $M_{r+1,j}$ to

3. construct all solutions.

3.1 the system $AX = a$ has a solution (consistent) $\Leftrightarrow$

$M_{i,n+1} = 0$ $r+1 \leq i \leq m$



$0 \neq 1$

$m-r$ entries in the last column.

3.2. variables x_j $t_i < j < t_{i+1}$ $(0 \le i \le r)$ may have any values

compute values of

$$x_{t_1}\ x_{t_2} \ldots x_{t_r}$$

loop:

For i from r to 1 do

$$x_{t_i} = M_{i\,n+1} + \sum_{j=t_i+1}^{n} x_j M_{ij}$$

(mod 2 arithmetic)

solutions of a consistent system $Ax=a$

$r = \text{rank}(A)$

$= 2^{n-r}$

Example. $m = n = 4$

$$\underset{A}{\left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right)} \underset{x}{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}} = \underset{a}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}}$$

augment A by a

$$M = \left(\begin{array}{cccc|c} \boxed{1} & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \xrightarrow{\substack{r=0 \\ t_2=0 \\ M_{11}=1}} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 0 & \boxed{1} & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

$r=1,\ t_2=1$

$M_{22}=1$

$$\rightarrow \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & \boxed{0} & \boxed{1} & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \rightarrow \begin{array}{l} r=2,\ t_2=2 \\ M_{34}=1 \end{array} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & \boxed{1} \\ 0 & 0 & 0 & 0 & \boxed{0} \end{array}\right)$$

t_1' t_2'' t_3''

$r=3,\ t_2=4$

system is consistent.

solutions $2^{4-3} = 2$

$t_2'' < 3 < t_3''$ $\Rightarrow$ x_3 may have any value

x_1, x_2, x_4 are to be computed.

$$x_4 = M_{35} + \sum_{j=5=t_3+1}^{4} x_j M_{3j} = M_{35} = 1$$

(t_3'')

$x_3 = 0$

$$x_2 = M_{25} + \sum_{j=3=t_2+1}^{4} x_j M_{2j} = 1 + \overset{x_3}{0} \cdot M_{23} + \overset{x_4}{1} \cdot M_{24} = 0$$

(t_2'')

$$x_1 = M_{15} + \sum_{j=2=t_1+1}^{4} x_j M_{1j} = 1 + 0 \cdot \overset{0}{M_{12}} + 0 \cdot \overset{1}{M_{13}} + 1 \cdot \overset{1}{M_{14}} = 0$$

$\Rightarrow$ solution $x_1 x_2 x_3 x_4 = 0001$

$x_4 = 1$

$x_3 = 1$

$\Rightarrow x_2 = 1 \Rightarrow x_1 = 1$

$\Rightarrow$ solution $x_1 x_2 x_3 x_4 = 1111$