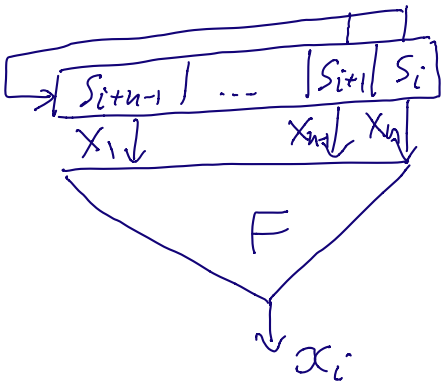
Algebraic Cryptanalysis.

Find cipher key (LFSR initial state)
by solving a system of algebraic
equation (in polynomial form)

Filter Generator



$$p(x) = x^n + c_1 x^{n-1} + \dots + c_n$$

problem (given $x^N = x_0 x_1 \dots x_{N-1}$
know pl-text attack sc.)
find initial state $(s_{n-1} \dots s_1 s_0)$

Construct system of equations !

$$(*) \begin{cases} x_i = F(s_{i+n-1} \dots s_{i+1} s_i) = F\left(\underbrace{(s_{n-1} \dots s_1 s_0) A^i}_{p(x)}\right) \\ A \text{ companion matrix to } p(x) \end{cases}$$

write equations $(*)$ with polynomials
(ANF for $F = F(x_1 \dots x_n)$)

algebraic degree of the equations.

assume $\deg F = d \Rightarrow$ every equation

in (*) is of degree d.

Lemma $F(X) = F(X_1, \ldots, X_n)$ Boolean function

A non-singular matrix of size $n \times n$.

Then $\deg F(X) = \deg F(X \cdot A)$

Proof. 1) $\deg F(X \cdot A) \le \deg F(X)$ for any matrix A.

Why?

ANF $F(X_1 \ldots X_n) = X_1 X_2 \ldots X_d + \ldots + X_{i_1} \ldots X_{i_6} + \ldots$

$F(\bar{x})$

$$F(X \cdot A) = \left(\sum_{i=1}^{n} X_i a_{i1}\right)\left(\sum_{i=1}^{n} X_i a_{i2}\right) \ldots \left(\sum_{i=1}^{n} X_i a_{id}\right) + \ldots$$

$$A = (a_{ij})_{1 \le i,j \le n}$$

expand brackets to get ANF for $F(X \cdot A)$

every monomial is of length $\le d$ (term, product of variables like $X_i X_{2_1} \ldots$)

$\Rightarrow$ $\deg F(X \cdot A) \le \deg F(X)$.

2) $\deg F(XA) \geq \deg F(X)$.

$\deg F(XA) \geq \deg F((XA^{-1})A) = \deg F(X)$

(A non-singular)

$\Rightarrow \quad \deg F(X \cdot A) = \deg F(X)$

$\Rightarrow$ (*) all polynomials are of degree $d \leq \deg F(X)$.

if $d \geq 2 \Rightarrow$ system of non-linear equations

$d = 1$ linear equations

Why non-linear equations are difficult?

lin. equations:

$$\begin{cases} X_1 + X_2 = 1 \\ X_1 + X_3 + X_4 = 0 \\ \dots \end{cases}$$

eliminate $X_1 = X_2 + 1$ from all other equations

$$\Rightarrow \begin{cases} X_1 + X_2 = 1 \\ X_2 + X_3 + X_4 = 1 \\ \dots \end{cases}$$ again linear

non-linear equations

$$\begin{cases} X_1 \cdot X_2 + X_3 = 1 \\ X_3 \cdot X_4 + X_1 + X_2 = 0 \\ \dots \end{cases}$$ (quadratic)

eliminate $X_3 = 1 + X_1 \cdot X_2$ from other equations:

$$\begin{cases} X_1 X_2 + X_3 = 1 \\ X_1 \cdot X_2 \cdot X_3 + X_1 + X_2 + X_4 = 0 \\ \dots \end{cases}$$

non-linear again, degree of the polynomials is growing. (cubic)

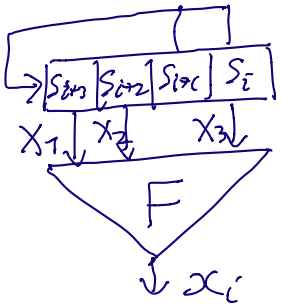
$\Rightarrow$ # terms (monomials) is growing rapidly

Linearization Attack.

reduces non-linear to linear.

1) denote all non-linear terms (monomials) as new variables.

2) use elimination to solve



Example.

$X^4 + X + 1$

$F(X_1 X_2 X_3) = X_1 + X_2 + X_1 X_3$

$\deg F = 2 = d$.

$x^{10} = 0110001011$

find $S_3 S_2 S_1 S_0$

construct system of non-lin. equations

$\vee$

$$\begin{cases} x_0 = S_3 + S_2 + S_3 \cdot S_0 = F(S_3 S_2 S_1 S_0) \\ x_1 = (S_0 + S_1) + S_3 + (S_1 + S_0) \cdot S_1 = F(S_0 + S_1\ S_3\ S_2\ S_1) \end{cases}$$

$$\begin{cases} \dots \\ x_g = s_0 + (s_0+s_1+s_2+s_3)(s_1+s_3) = F((s_3,s_2,s_1,s_0)A) \end{cases}$$

$$A = \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&1 \\ 1&0&0&0 \end{pmatrix}$$

expand brackets and use $s_i^2 = s_i$ as $s_i = 0$ or 1.

new variables s_3, s_2, s_1, s_0

$T = s_0 s_1$ $\quad V = s_0 s_3$ $\quad R = s_1 s_3$

$U = s_0 s_2$ $\quad W = s_1 s_2$ $\quad Z = s_2 s_3$

now we have 10 variables $= 4 + 6$

write lin. system

$$\begin{cases} \begin{cases} 0 = s_3 + s_2 + V \\ 1 = s_0 + s_3 + T \\ 1 = s_0 + W \\ 0 = s_1 + Z \\ 0 = s_2 + V + R \\ 0 = s_1 + s_3 + U + W + T \\ 1 = s_1 + s_0 + s_2 + W + R + Z \\ 0 = s_2 + s_3 + s_1 + V + U + W + R + Z \\ 1 = s_3 + s_0 + s_2 + V + U + W + T + Z \\ 1 = s_0 + s_1 + s_3 + V + W + T + Z \end{cases} \end{cases}$$

var. $= 10$

equations $= 10$

solve by elimitation, rank $= 10$

solutions is $2^{10-10} = 1$

solution is unique

$$T=U=V=W=R=Z=\underbrace{S_3=S_2=S_1=0}\quad S_0=1$$

$\Rightarrow$ initial state is (0001).

Complexity of the method

d alg. degree of the polynomials

variables after linearization

$$\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\dots+\binom{n}{d}=D$$

↑ # monomials of deg = 2

N # equations (key-stream size in the example)

$$\#\text{ solutions} = 2^{D-R}$$

R = rank of the system matrix.

unique solution if $R=D\leq N$

may have

$\Rightarrow N \gtrsim D$

if the solution is not unique, one runs over all 2^{D-R} solutions to the system after linearization.

Extended Linearization (XL) Attack.

system of polynomial equations:

$$(*)\quad \begin{cases} f_1(x_1 \cdots x_n) = 0 \\ \cdots \\ f_m(x_1 \cdots x_n) = 0 \end{cases}$$

Boolean polynomials. Chose parameter c

construct a new equation system

$$(**)\quad \{ \underbrace{x_1^{i_1} \cdots x_n^{i_n} \cdot f_i = 0}_{\text{monomials}} \leftarrow \text{incorporates } \{f_i = 0$$

s.t. $\deg(x_1^{i_1} \cdots x_n^{i_n} f_i) \leq c$

$i_1 + \cdots + i_n + \deg f_i \leq c$

$(*)$ is equivalent to $(**)$

(they have the same solutions)

- $x_1 \cdots x_n$ solution to $(*)$, that is a sol. to $(**)$.
- $x_1 \cdots x_n$ $(**)$ that is a sol. to $(*)$

because $(*) \subseteq (**)$

Solve (**) with linearization/elimination.

Complexity

D_c # monomials in polyn. (**)

$$= \sum_{i=1}^{c} \binom{n}{i}$$ (exclude monomial 1)

R_c rank after (**) is linearized.

complexity $D_c^3 + 2^{D_c - R_c} \approx 1$

- D_c^3: cost of elimination
- $2^{D_c - R_c} \approx 1$: search over all solutions to linearized (**)

Fact. if (*) has a low # solutions there is c s.t. $\underline{R_c \approx D_c}$

$\Rightarrow$ compl. is D_c^3

c is difficult to compute,

Example.

$$\begin{cases} x_1 x_2 + x_3 = 0 \\ x_2 x_3 + x_3 + x_1 = 1 \\ x_1 x_3 + x_2 = 0 \end{cases}$$

apply pl. linearization

$u = x_1 \cdot x_2$
$v = x_2 \cdot x_3$
$w = x_1 \cdot x_3$

$$\Rightarrow \begin{cases} u + x_3 = 0 \\ v + x_3 + x_1 = 1 \\ w + x_2 = 0 \end{cases}$$

$\Rightarrow 2^{6-3} = 8$ solutions.

apply. XL , $c=3$

mul. by x_1

$$x_1x_2 + x_1x_3 = 0$$
$$x_1x_2x_3 + x_1x_3 + x_1 = x_1$$
$$x_1x_3 + x_1 \cdot x_2 = 0$$

mult. by x_2

$$x_2x_2 + x_2x_3 = 0$$
$$x_2x_3 + x_2x_3 + x_1x_2 = x_2$$
$$x_1x_2x_3 + x_2 = 0$$

mult. by x_3

$$x_1x_2x_3 + x_3 = 0$$
$$x_2x_3 + x_3 + x_1x_3 = x_3$$
$$x_1x_3 + x_2x_3 = 0$$

initial equations

$$x_1x_2 + x_3 = 0$$
$$x_2x_3 + x_3 + x_1 = 1$$
$$x_1x_3 + x_2 = 0$$

new var. $x_1x_2x_3,\ x_1x_2,\ x_2x_3,\ x_1x_3$

sol. system of 12 equations in 7 var.

rank $= 6 \Rightarrow 2^{7-6} = 2$ solutions

$$x_1x_2x_3 = x_1x_2 = x_1x_3 = x_2x_3 = x_2 = x_3,\ x_1 = 1$$

2 solutions to the initial equations

$$x_1x_2x_3 = \begin{matrix} 1\,0\,0 \\ 1\,1\,1 \end{matrix}$$