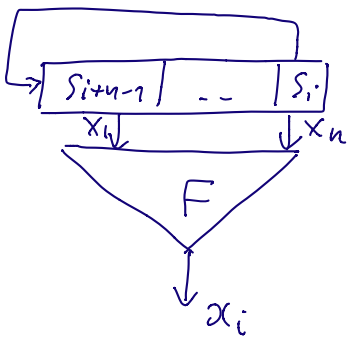
Annihilator Attack.



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

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

system of equations

$$\begin{cases} x_i = F(s_{i+n-1} \dots s_i) = F(S \cdot A^i) \\ i = 0, \dots, N-1 \end{cases}$$

(S: initial state)

idea is to reduce alg. degree of the equations.

motivation. $F(X_1 \dots X_n) = X_1 X_2 X_3 \dots X_i + X_1 + \dots + X_n$

identity $(X_1 + X_2)(X_1 + X_2) = X_1^2 + X_1 X_2 + X_1 X_2 + X_2^2 =$

$= X_1 X_2 + X_1 X_2 = 0$

$(X_1 + X_2) \cdot F = (X_1 + X_2) X_1 X_2 \dots X_i + (X_1 + X_2)(X_1 + \dots + X_n) =$

$= (X_1 + X_2)(X_1 + \dots + X_n)$ of degree 2.

multiply every equation by $(X_1 + X_2)(SA^i)$

$\Rightarrow$ eq. system of a lower degree.

easier to solve with linearization.

---

let $F = F(X_1 \dots X_n) \neq 0$ Boolean function

$G = G(X_1 \dots X_n) \neq 0$ is called annihilator for F

if $G \cdot F = 0$

trivial annihilators

$$F(F+1) = F^2 + F = F + F = 0$$

$\Rightarrow$ $F+1$ ann. for F $\quad \deg F+1 = \deg F$, $F \neq 0,1$

F ann. for $F+1$

Examples. $F(X_1 \dots X_4) = \underbrace{X_1X_2X_4 + X_2X_3X_4}_{} + X_2X_4 + X_2X_3 + X_1X_4 + X_1 + X_2 + X_3 + X_4$

$\deg F = 3$

$G_0 = X_1 X_2 + X_3 \cdot X_4$

$\Rightarrow G_0 \cdot F = 0$ by Lecture Notes

$G_1 = X_1 X_4 + X_1 X_3 + X_3 + X_4$

$\Rightarrow G_1 \cdot (F+1) = 0$ by Lect. Notes

$\deg G_0, \deg G_1 = 2 < \deg F = 3$

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

Then there exist $G = G(X_1 \dots X_n)$, $H = H(X_1 \dots X_n)$

s.t.

1) $G \cdot F = H$
2) $\deg G, \deg H \leq \left\lceil \frac{n}{2} \right\rceil$ $\quad (\lceil 0.7 \rceil = 1)$
3) at least one of G, H is not 0.

Proof. $\quad G = \sum_{m : \deg m \leq \lceil \frac{n}{2} \rceil} c_m m$

c_m ← unknown coeff.

m ⇖ monomial (product of variables like $X_1 X_2$)

$$H = \sum_{m:\deg m \le \lceil \frac{n}{2} \rceil} d_m m$$

(d_m: unknown coeff.)

construct a system of linear equations

$GF = H \iff$

$$T = \underbrace{\sum_{m:\dots} c_m \cdot m \cdot F + \sum_{m:\dots} d_m \cdot m}_{\text{Boolean function in } n \text{ var. in ANF}} = 0$$

$\iff$ all coeff. of T in ANF are 0

$\iff$ c_m, d_m variables in a system of 2^n homogeneous lin. equation. (m of degree $\le \lceil \frac{n}{2} \rceil$)

($x_1 + x_2 = 0$, $x_3 = 0$, ...)

Fact from Linear Algebra.

[if # variables > # equations
$\Rightarrow$ hom. lin. system has a non-zero solution.]

$$\#\text{variables} = 2 \cdot \sum_{i=0}^{\lceil n/2 \rceil} \binom{n}{i}$$

($\binom{n}{i}$: # monomials of degree i in n var.)

equations $= 2^n$

check that

$$2 \cdot \sum_{i=0}^{\lceil n/2 \rceil} \binom{n}{i} > 2^n \qquad (*)$$

combinatorics.

1) $n = 2k$

$$\binom{n}{k}$$

lhs (*) $\quad 2 \cdot \sum_{i=0}^{k} \binom{n}{i}$

rhs (*) $\quad 2^n = \binom{n}{0} + \dots + \binom{n}{k} + \underbrace{\binom{n}{k+1}}_{\binom{n}{k-1}} + \underbrace{\binom{n}{k+2}}_{\binom{n}{k-2}} + \dots + \underbrace{\binom{n}{n}}_{\binom{n}{0}}$

$\binom{n}{i} = \binom{n}{n-i}$

$\Rightarrow$ (*) is correct for $n = 2k$.

2) $n = 2k+1$

lhs (*) $\quad 2 \cdot \sum_{i=0}^{k+1} \binom{n}{i}$

rhs (*) $\quad 2^n = \binom{n}{0} + \dots + \binom{n}{k+1} + \underbrace{\binom{n}{k+2}}_{\binom{n}{k-1}} + \underbrace{\binom{n}{k+3}}_{\binom{n}{k-2}} + \dots + \underbrace{\binom{n}{n}}_{\binom{n}{0}}$

$\Rightarrow$ (*) correct for $n = 2k+1$

system of lin. Eqs a non-zero solution $\Rightarrow$ G, H non-zero, $\deg G, \deg H \le \lceil \frac{n}{2} \rceil$

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

G, H linear s.t. $\boxed{G \cdot F = H}$

$\deg G, \deg H = 1 < \lceil \frac{n}{2} \rceil = 2$ as $n = 3$

$G = c_1 X_1 + c_2 X_2 + c_3 X_3$ $\quad c_i \leftarrow$ unknowns

$H = d_1 X_1 + d_2 X_2 + d_3 X_3$ $\quad d_i \swarrow$

$$(c_1 X_1 + c_2 X_2 + c_3 X_3)(X_1 X_2 X_3 + X_1 + X_2) = d_1 X_1 + d_2 X_2 + d_3 X_3$$

$$(c_1+c_2+c_3) X_1 X_2 X_3 + (c_1+d_1) X_1 + (c_2+d_2) X_2 + (c_1+c_2) X_1 X_2 + c_3 X_1 X_3 + c_3 X_2 X_3 + d_3 X_3 = 0$$

$\Rightarrow$ system of lin. equations

$$\begin{cases} c_1+c_2+c_3 = 0 \\ c_1+d_1 = 0 \\ c_2+d_2 = 0 \\ c_1+c_2 = 0 \\ c_3 = 0 \\ c_3 = 0 \\ d_3 = 0 \end{cases} \iff \begin{array}{l} c_1+c_2=0 \\ c_1+d_1=0 \\ c_2+d_2=0 \\ c_3=d_3=0 \end{array}$$

non-zero solution is

$c_1 = c_2 = d_1 = d_2 = 1$

$c_3 = d_3 = 0$

$\Rightarrow$ $G = X_1 + X_2$, $H = X_1 + X_2$

$(X_1 + X_2) \cdot F = X_1 + X_2$

Corollary F or $F+1$ has an annihilator of degree $\leq \lceil \frac{n}{2} \rceil$.

Proof. $G \cdot F = H$ $\quad \deg G, \deg H \leq \lceil \frac{n}{2} \rceil$

at least G or H is non-zero.

1) $H \neq 0$

$H \cdot F = G \cdot F \cdot F = G \cdot F = H$

as $F^2 = F$

$\Rightarrow H(F+1) = 0 \Rightarrow H$ ann. for $F+1$

$\deg H \leq \lceil \frac{n}{2} \rceil$.

2) $H = 0 \Rightarrow G \neq 0$

$G \cdot F = 0 \Rightarrow G$ ann. for F

$\deg G \leq \lceil \frac{n}{2} \rceil$.

Remark. assume that $H \neq 0$, $G \neq H$

$\Rightarrow H(F+1) = 0$

$(G+H)F = 0$

as. $(G+H) \cdot F = G \cdot F + H \cdot F = H + H \cdot F = H(1+F) = 0$

↑ non-zero $\quad \deg G+H \leq \lceil \frac{n}{2} \rceil$.

Back to the Cryptanalysis $\begin{cases} G_0 \text{ ann. for } F \\ G_1 \text{ ann. for } F+1 \end{cases}$

$\begin{cases} x_i = F(S \cdot A^i) \quad i = 0, \dots, N-1 \end{cases}$

1) $x_i = 1$ multiply the equation by $G_0(SA^i)$

$$G_0(SA^i) = (F \cdot G_0)(SA^i) = 0$$

a lower degree equation if $\deg G_0 < \deg F$.

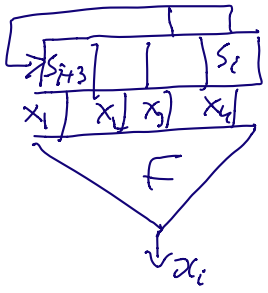
2) $x_i = 0$ multiply the equation by $G_1(SA^i)$

$$1 = (1+F)(SA^i)$$

$$\Rightarrow \quad G_1(SA^i) = \underbrace{\big((1+F)\cdot G_1\big)}_{=0}(SA^i) = 0$$

a lower degree equation of $\deg G_1 < \deg F$.

Example.



$P(x) = x^4 + x + 1$

$x^{10} = 1111\ 101001$

$F = x_1x_2x_3 + x_2x_3x_4 + \dots + x_4$

system of 10 cubic equations

$$\{ x_i = F(S \cdot A^i) \quad i = 0, \dots, 9$$

after linearization $\binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 14$ variables.

$\#$ eq. $= 10 \Rightarrow \#$ solutions $\geq 2^{14-10} = 16$

use annihilator $G_0 \cdot F = 0 \quad G_0 = x_1x_2 + x_3x_4$

$G_1(F+1) = 0 \quad G_1 = x_1x_4 + x_1x_3 + x_3x_4$

new system $\begin{cases} G_0(SA^i) = 0 & i \in \{0,1,2,3,4,6,9\} \\ & x_i = 1 \\ G_1(SA^i) = 0 & i \in \{5,7,8\} \\ & x_i = 0 \end{cases}$

linearization

variables $\binom{4}{1} + \binom{4}{2} = 10$

eq. $= 10$

rank of the system is 10 $\Rightarrow$ unique solution. (0001).