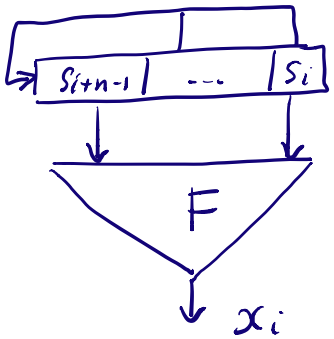
Fast Correlation Attack

apply to Filter Generator based stream cipher.



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

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

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

1. Find a good (best) affine approximation to $F(X_1 \dots X_n)$

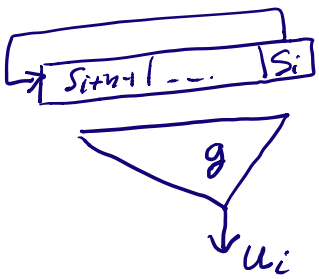
maximize $p = P_r(F = g)$ ← affine Boolean function

$g = a_1 X_1 + \dots + a_n X_n + b$

can assume $b = 0$. otherwise, $b = 1$

change $\begin{cases} F \leftarrow F + 1 \\ x_i \leftarrow x_i + 1 \end{cases}$ xor's

2. idea



u_i known lin. functions in $s_{n-1} \dots s_1 s_0$

$v_k = u_k + x_k$, $k = 0, \dots, N-1$

x_k ← known key-stream

v_k ← new variables

$p = P_r(v_k = 0)$ a priori probability.

compute a posteriori probabilities

$$p_k = P_r(v_k = 0 \,/\, \text{key-stream})$$

↑ new information about Filter Generator.

the probabilities p_k larger than p.

take $\{i_1 \dots i_{n_1}\}$ with largest p_k $\quad k \in \{i_1 \dots i_{n_1}\}$

$n_1 \geq n$

take system of n_1 lin. equations

$$\begin{cases} v_{i_1} = u_{i_1} + x_{i_1} \\ \dots \\ v_{i_{n_1}} = u_{i_{n_1}} + x_{i_{n_1}} \end{cases}$$

$$p^* = \min_{k \in \{i_1 \dots i_{n_1}\}} p_k \Rightarrow q^* = 1 - p^*$$

$\Rightarrow$ weight $(\text{correct}(v_{i_1} \dots v_{i_{n_1}})) \leq q^* \cdot n_1$.

$q^* < q \Rightarrow q^* n_1 < q \cdot n_1$

$\Rightarrow$ advantage over Affine Approximation Attack.

Sparse Linear Relations

$|s_{i+n-1}| \dots |s_i| \rightarrow$ $\quad s_0 s_1 \dots s_{N-1}$, N

$$s_{i+m} + d_1 s_{i+m-1} + \dots + d_m s_i = 0 \qquad (*)$$

non-zero $d_1 \dots d_m$ is low

$(*)$ is sparse.

Example. $f(x) = x^n + x^e + 1$ trinomial

$s_{i+n} + s_{i+e} + s_i = 0 \quad i = 0, 1, \dots$

sparse linear relation.

Fact. (*) holds for every $i = 0, 1, \ldots$

$\Leftrightarrow$ $f(x) \mid X^m + d_1 \cdot X^{m-1} + \ldots + d_m$.

In order to construct sparse relations (*) we find low weight polynomials s.t.

Example. $f(x) = X^n + X^\ell + 1$

$f(x) \mid f^{2^r}(x) = X^{n \cdot 2^r} + X^{\ell \cdot 2^r} + 1$ as mod 2 arithmetic. $\Leftarrow (a+b)^2 \equiv a^2 + b^2$.

of low weight.

relations $S_{n \cdot 2^r + i} + S_{\ell \cdot 2^r + i} + S_i = 0$

$i = 0, 1, \ldots$

$f(x) = X^4 + X + 1$

sparse relations

$S_4 + S_1 + S_0 = 0$

$S_5 + S_2 + S_1 = 0$

$S_6 + S_3 + S_2 = 0$

$\ldots$

$f^2(x) = X^8 + X^2 + 1$ $S_8 + S_2 + S_0 = 0$

$S_9 + S_3 + S_1 = 0$

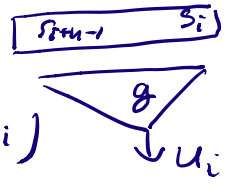
$S_{10} + S_4 + S_2 = 0$

$\ldots$

$f^4(x) = X^{16} + X^4 + 1$ $\ldots$

$u_i = a_1 \cdot S_{i+n-1} + a_2 S_{i+n-2} + \ldots + a_n S_i$

$\nwarrow$ ein Funktion on $(S_{i+n-1} \ldots S_i)$



if (*)

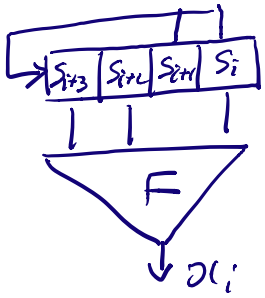
$u_{i+m} + d_1 u_{i+m-1} + \ldots + d_m u_i = 0$

d_m $u_0 = a_1 S_{n-1} + \ldots + a_n \cdot S_0$

d_{m-1} $u_1 = a_1 S_n + \ldots + a_n S_1$

$i=0$		
d_1	$u_m = a_1 s_{1+m-1} + \dots + a_4 s_m$	
1	$u_{m+1} = a_1 s_{1+m} + \dots + a_4 s_{m+1}$	
	$0 = 0 + \dots + 0$	

Example of the Attack.



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

F as in the previous example (Affine Approx. Attack).

$x_0 x_1 x_2 x_3 x_4$

task: given key-stream $x^{12} = 011000101110$

find $s_3 s_2 s_1 s_0$

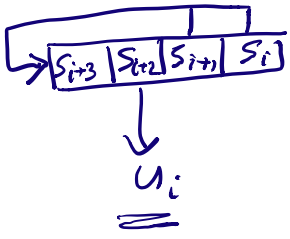
system of lin. equations as in AA

$$\begin{cases} v_0 = x_0 + u_0 \\ v_{11} = x_{11} + u_{11} \end{cases}$$

$g = x_2$

$P_2(v_i = 0) = 3/4$

$P_2(F = x_2) = \frac{3}{4}$



$x^4 + x + 1$

$$\begin{cases} v_4 + v_1 + v_0 = x_4 + x_1 + x_0 + \underbrace{u_4 + u_1 + u_0}_{0} \\ v_5 + v_2 + v_1 = x_5 + x_2 + x_1 + \underbrace{u_5 + u_2 + u_1}_{0} \\ \dots \end{cases}$$

$$\Rightarrow \begin{cases} v_4 + v_1 + v_0 = x_4 + x_1 + x_0 = 1 \\ \dots \\ v_{11} + v_8 + v_7 = x_{11} + x_8 + x_7 = 1 \end{cases}$$

$x^8 + x^2 + 1$

$$\begin{cases} v_8 + v_2 + v_0 = x_8 + x_2 + x_0 \\ \dots \end{cases}$$

$(v_{11} + v_5 + v_3 = x_{11} + x_5 + \dots)$ may be computed

Do that

$$(**)\quad \begin{cases} v_4 + v_1 + v_0 = 1 \\ v_5 + v_2 + v_7 = 0 \\ \dots \\ v_{11} + v_8 + v_7 = 1 \\ v_8 + v_2 + v_0 = 0 \\ v_9 + v_3 + v_1 = 0 \\ v_{10} + v_4 + v_2 = 0 \\ v_{11} + v_5 + v_3 = 0 \end{cases}$$

depends on the key-stream

compute $p_k = P_r(v_k = 0 / (**))$

analyse $(**)$

$k = 0, 1, \dots, 11$

compute m_k # relations $(**)$ where v_k occurs

R_k # relations where v_k occurs and zRS is 0

e.g. $k = 1$ v_1 is in $(**)$

$m_1 = 3, \; R_1 = 2$

fill the table

k	0	1	2	3	4	5	6	7	8	9	10	11
m_k	2	3	4	4	4	4	3	3	3	2	2	2
R_k	1	2	4	4	2	3	3	2	1	2	2	1
P_k	0.75	0.83	0.95	0.95	0.75	0.89	0.93	0.83	0.64	0.89	0.89	0.75

formula for computing P_k

$$= \frac{3}{4}$$

p a priori probability $= \frac{1}{4}$

t # LFSR taps $= 2$

1. $S = S(P,t)$ Why correct?

$S(P,1) = P$

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

2.

$$P_K = \frac{p \cdot S^{R_K}(1-S)^{m_K - R_K}}{p \cdot S^{R_K}(1-S)^{m_K - R_K} + (1-p)\, S^{m_K - R_K}(1-S)^{R_K}}$$

define set $\{2,3,5,6,10\}$

$p^* = \min_{K \in \{2,3,5,6,10\}} \{P_K\} = 0.89$

$q^* = 0.11$

system of lin. equations.

$$\begin{cases} v_2 = u_2 + x_2 \\ v_3 = u_3 + x_3 \\ v_5 = u_5 + x_5 \\ v_6 = u_6 + x_6 \\ v_{10} = u_{10} + x_{10} \end{cases}$$

average weight (correct $(v_2 v_3 \ldots v_{10})$) $\leq q^* n_1 = 0.11 \cdot 5 = 0.55$

weight to try $0, 1, 2, \ldots$

define $u_i = (s_3 s_2 s_1 s_0) \begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&1 \\ 1&0&0&0 \end{pmatrix}^i \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

companion matrix to $x^4 + x + 1$

$u_2 = s_0 + s_1$

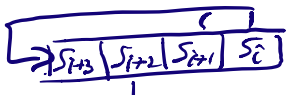
$u_3 = s_1 + s_2$

$u_5 = s_0 + s_1 + s_3$

$u_6 = s_0 + s_2$

$u_i = (s_{i+3} s_{i+2} s_{i+1} s_i) \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = s_{i+2}$

$u_{10} = s_0 + s_1 + s_2 + s_3$



$u_i = g(s_{i+3}, s_i)$

$= s_{i+2}$

$g = x_2$

$g = a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4$

$= x_2$

$u_i = (s_{i+3} \; s_i) \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$

$\Rightarrow$ system

$$\begin{aligned} v_2 &= s_0 + s_1 + 1 \\ v_3 &= s_1 + s_2 + 0 \\ v_5 &= s_0 + s_1 + s_2 + 0 \\ v_6 &= s_0 + s_2 + 1 \\ v_{10} &= s_0 + s_1 + s_2 + s_3 + 1 \end{aligned}$$

5 equations in 4 variables

try LRS

1) $v_2 v_3 v_5 v_6 v_{10} = 00000$

solve the system

solution $s_3 s_2 s_1 s_0 = 1110$

check solution on gen. key-steam

0110011 ...

differs from available

$\Rightarrow$ guess was wrong!

2) $v_2 v_3 v_5 v_6 v_{10} = 00100$

correct solution $s_3 s_2 s_1 s_0 = 0001$.