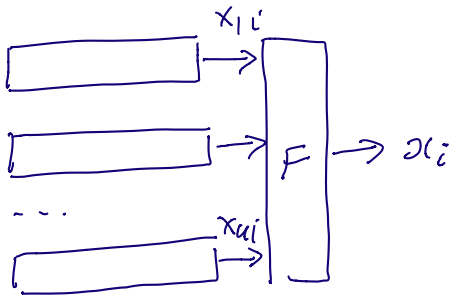
Correlation Immune Boolean Function.



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

recover LFSRs initial states.

correlation attack is based

$$\varphi = \varphi(X_1 \ldots X_k) \qquad k < n$$

and $P_2(F = \varphi) \neq \frac{1}{2}$

$F(X_1 \ldots X_n)$ balanced if F has

2^{n-1} 0 values

2^{n-1} 1 values

Definition F called m-balanced $(0 \leq m < n)$ if any $X_{i_1} \ldots X_{i_m}$ variables

$a_1 \ldots a_m$ constants, $v_i \in$

$F(X_1 \ldots \underset{i_1}{a_1} \ldots \underset{i_m}{a_m} \ldots X_n)$ is balanced.

(m^{th} order correlation immune).

Examples. 1) $F(X_1 \ldots X_n) = X_1 + X_2 + \ldots + X_n$

$(n-1)$-balanced.

$F(a_1, \ldots, a_{n-1}, X_n) = \underbrace{(a_1 + a_2 + \ldots + a_{n-1})}_{\text{constant}} + X_n$

non-constant Boolean function in X_n

2) stream cipher "Grain"

$$h(x_0x_1x_2x_3x_4) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4.$$

h is 1-balanced but is not 2-balanced. ($n=5$, $m=4$; if yes $\deg h \le 5-2-1=2$ $\Rightarrow$ h is not 2-balanced)

Theorem

1) $F = F(x_1 \dots x_n)$ m-balanced $\Rightarrow$ F is k-balanced, $0 \le k \le m$.

2) F m-balanced

$$\deg F = \begin{cases} 1 \\ \le n-m-1 \end{cases}$$

3) F m-balanced $\Leftrightarrow$ $P_2(F = \varphi(x_{i_1} \dots x_{i_k})) = \frac{1}{2}$ any $k \le m$ any $\varphi(x_{i_1} \dots x_{i_k})$

Proof. 1) $x_1, \dots, x_k = a_1, \dots, a_k$

$F' = F(a_1, \dots, a_k, x_{k+1} \dots x_n)$ is balanced

$$P_2(F'=1) = \sum_{b_{k+1} \dots b_n} P_2(x_{k+1} \dots x_n = b_{k+1} \dots b_n) \cdot P_2(F' = 1 / x_{k+1} \dots x_n = b_{k+1} \dots b_n)$$

complete probability formula

$$= \sum_{b_{k+1}\dots b_m} \underbrace{P_2(X_{k+1}\dots X_m = b_{k+1}\dots b_m)}_{\frac{1}{2^{m-k}}} \cdot \underbrace{P_2(F(a_1\dots a_k b_{k+1}\dots b_m X_{m+1}\dots X_n)=1)}_{\frac{1}{2}\ \ F \text{ is } m\text{-balanced}}$$

$$= \frac{1}{2} \Rightarrow F' \text{ balanced}$$

$\Rightarrow F$ is k-balanced.

2) **Lemma.** $F = F(X_1 \dots X_n)$, $n \geq 2$

balanced $\Rightarrow$ $\deg F \leq n-1$.

Proof. $F = (F(0), F(1), \dots, F(2^n-1))$

$C = (c_0, c_1, c_2, \dots, c_{2^n-1})$ ANF coeff.

$$F = c_0 + c_1 X_n + c_2 X_{n-1} + c_3 X_{n-1}X_n + \dots + c_{n-1} X_1 X_2 \dots X_n$$

$$C = F \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{[n]}}_{2^n \times 2^n} = F \cdot \left| \quad * \quad \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix} \right. \Rightarrow$$

$$c_{2^n-1} = \sum_{a=0}^{2^n-1} F(a) = 2^{n-1} \bmod 2 = 0 \text{ as } n \geq 2.$$

proof of 2)

if $\deg F = 1$ nothing to prove

let $\deg F = k \geq 2$ and $k \geq n-m$ by contrary

ANF for F = $\boxed{X_1 \cdot X_2 \cdots X_k}$ + ... + $X_{j_1} X_{j_2} \cdots X_{j_e}$ + ...

$X_{j_1} X_{j_2} \cdots X_{j_e} \neq X_1 \cdot X_2 \cdots X_k$

1) $e < k$

2) $e = k$ $\boxed{X_{j_1} X_{j_2} \cdots X_{j_e}}$ incorporates at least one variable in $\{X_{k+1} \cdots X_n\}$

fix $X_{k+1} \cdots X_n = a_{k+1} \cdots a_n$

$G = F(X_1 \cdots X_k a_{k+1} \cdots a_n) = \boxed{X_1 \cdot X_2 \cdots X_k} + \cdots + \overbrace{X_{j_1} \cdots X_{j_e}}^{e<k} + \cdots$

$\Rightarrow \deg G = k \geq 2$

G balanced $\Leftarrow$ contradiction with $k \geq n-m$ ($\boxed{n-k \leq m}$)

$\Rightarrow \boxed{k \leq n-m-1}$

$\Rightarrow$ F m-balanced

$\Rightarrow F$ k-balanced, $k \leq m$.

$\varphi = \varphi(X_1 \cdots X_k)$ $\quad 1/2^k$

$$Pr(F = \varphi) = \sum_{a_1 \cdots a_k} \overbrace{Pr(X_1 \cdots X_k = a_1 \cdots a_k)}^{\text{constant}} \times Pr(F(a_1 \cdots a_k X_{k+1} \cdots X_n) = \varphi(a_1 \cdots a_k))$$

$\sim \frac{1}{2}$ F k-balanced

$$= \sum_{a_1 \dots a_k} \frac{1}{2^k} \cdot \frac{1}{2} = \frac{1}{2}$$

$\Leftarrow$ if $\Pr(F = \varphi(x_{i_1} \dots x_{i_k})) = \frac{1}{2}$

any $k \le m$ any $\varphi(x_{i_1} \dots x_{i_k})$

then F m-balanced.

assume not F is not m-balanced

$\Rightarrow F(a_1 \dots a_m x_{m+1} \dots x_n)$ not balanced

construct $\varphi(x_1 \dots x_m)$ explicitly

$$\varphi(b_1 \dots b_m) = \begin{cases} 1 & \Pr(F(b_1 \dots b_m x_{m+1} \dots x_n) = 1) \ge \frac{1}{2} \\ & = \varphi(b_1 \dots b_m) \\ 0 & \Pr(F(b_1 \dots b_m x_{m+1} \dots x_n) = 0) > \frac{1}{2} \end{cases}$$

$b_i \in \{0,1\}$

well defined Boolean function.

Then

1) $\Pr(F(b_1 \dots b_m x_{m+1} \dots x_n) = \varphi(b_1 \dots b_m)) \ge \frac{1}{2}$

2) $\Pr(F(a_1 \dots a_m x_{m+1} \dots x_n) = \varphi(a_1 \dots a_m)) > \frac{1}{2}$

$F(a_1 \dots a_m x_{m+1} \dots x_n)$ is not balanced.

$$P_2(F=\varphi) =$$

$$\sum_{b_1 \dots b_m} \underbrace{P_2(X_1 \dots X_m = b_1 \dots b_m)}_{\frac{1}{2^m}} \; P_2(F(b_1 \dots b_m X_{m+1} \dots X_n) = \varphi(b_1 \dots b_m))$$

always $\geq 1/2$

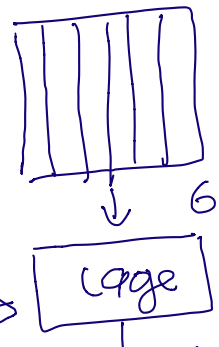
i.p. $b_1 \dots b_m = a_1 \dots a_m$ then $> 1/2$

$$> \frac{1}{2}$$

contradiction with $P_2(F=\varphi) = \frac{1}{2}$ ▨

$\Rightarrow$ m-balanced Boolean functions are good to construct some stream ciphers.

Hagelin



discrete function 6-bit → Latin alphabet is not 1-balanced.