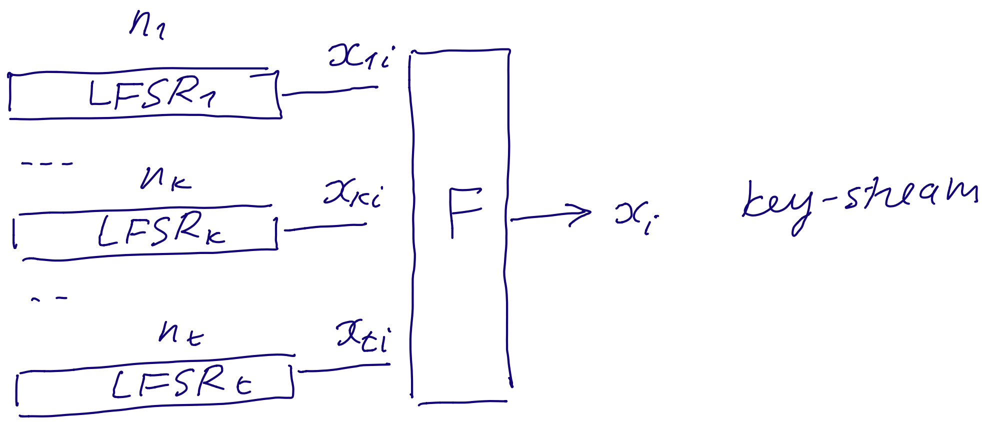
Correlation Attack for combiners



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

Problem given LFSRs initial states

find $S_1^0 \dots S_t^0$

brute force $(2^{n_1}-1)\dots(2^{n_t}-1) \approx \boxed{2^{n_1+\dots+n_t}}$

---

assume Boolean function

$\varphi = \varphi(X_1 \dots X_k)$, $k < t$

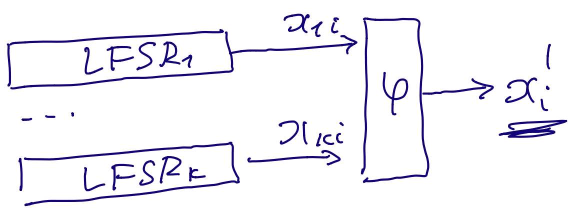
$F = F(X_1 \dots X_k \dots X_t)$

$P_r(\varphi = F) = q \neq \frac{1}{2}$ $q = \frac{1}{2} - \delta$, $\delta \neq 0$

δ called bias of the approximation $\varphi = F$

$0 < |\delta| < \frac{1}{2}$

construct another combiner



x_i, x_i' are correlated (dependent)

$\Pr(x_i = x_i') = \Pr(\varphi = F) = q \neq \frac{1}{2}$

Find initial states of $\underbrace{LFSR_1 \dots LFSR_k}_{S_1^0 \dots S_k^0}$

idea: guess initial states of LFSR's

$\underbrace{S_1 \dots S_k}$ current guess

generate x_i' on this guess

$\underbrace{v_i = x_i \oplus x_i'}$ $\quad i = 0, \dots, N-1$

available key-stream

depends on current guess

$\underbrace{v_0 v_1 \dots v_{N-1}}$

Two cases

1.) guess correct $S_1 \dots S_k = S_1^0 \dots S_k^0$

$\Pr(v_i = 0) = \Pr(x_i = x_i') = q = \frac{1}{2} - \delta$

$\Pr(v_i = 1) = p = \frac{1}{2} + \delta$

2.) guess incorrect $S_1 \dots S_k \neq S_1^0 \dots S_k^0$

x_i', x_i are independent

$\Pr(v_i = 0) = \Pr(x_i = x_i') = \frac{1}{2}$

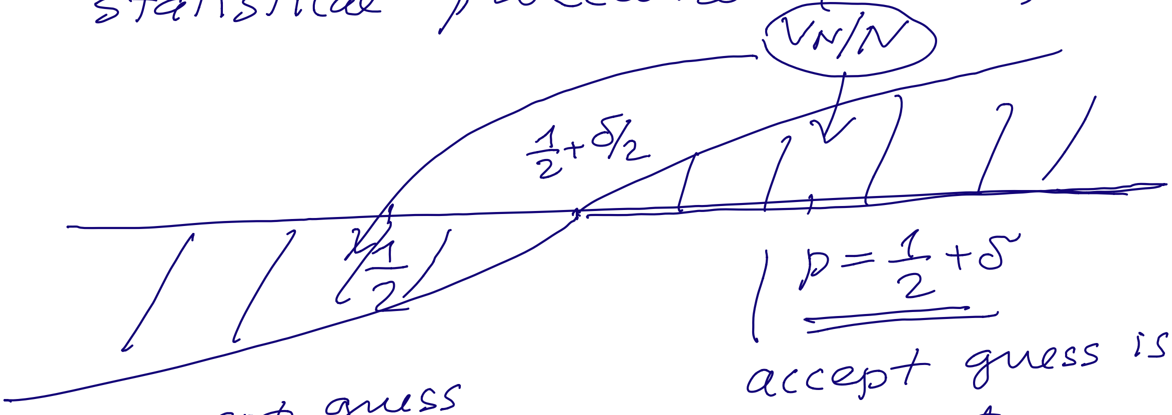
$\Pr(v_i = 1) = \frac{1}{2}$.

Algorithm

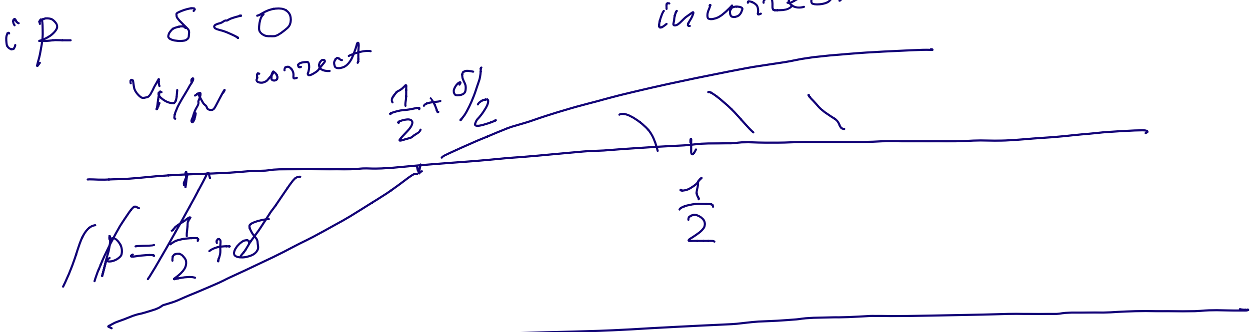
for each guess $S_1 \dots S_k$ compute

$$V_N = \sum_{i=0}^{N-1} v_i \quad \# \ 1 \text{ in } \underbrace{v_0 v_1 \dots v_{N-1}}$$

statistical procedure ($\delta > 0$)



if $\delta < 0$



Errors

$$\underline{\underline{\alpha_N}} = P_r\left(\text{accept guess correct} \,/\, \underbrace{\text{it was incorrect}}_{}\right) \quad S_1 \dots S_k$$

$$\underline{\underline{\beta_N}} = P_r\left(\text{accept guess incorrect} \,/\, \text{it was correct}\right) \quad S_1 \dots S_k$$

Meaning of $\alpha_N, \underline{\underline{\beta_N}}$

$$1-\beta_N = P_r\left(\text{accept guess correct} \,/\, \text{correct}\right)$$

success probability

β_N failure prob.

$$\boxed{\alpha_N \cdot \boxed{2^{n_1+\dots+n_k}}}$$ # survived incorrect initial states of $LFSR_1, \dots, LFSR_k$.

What to do next?

guess the rest of initial states

$$\boxed{\alpha_N \cdot 2^{n_1+\dots+n_k}} \cdot \boxed{2^{n_{k+1}+\dots+n_t}} =$$

$$= \underbrace{\alpha_N 2^{n_1+\dots+n_t}}_{\text{with correlation attack.}} < \underbrace{2^{n_1+\dots+n_t}}_{\uparrow \text{ brute force}}$$

How large N to make α_N, β_N small?

$\delta > 0$ $\qquad Pr(v_i = 1) = p = \frac{1}{2} + \delta$, $\delta > 0$

$$\alpha_N = Pr(\text{accept correct}/\text{incorrect}) =$$

$\Updownarrow$

$Pr(v_i = 1) = \frac{1}{2}$

$$= Pr\left(\frac{V_N}{N} \geq \frac{1}{2} + \delta/2 \,/\, Pr(v_i = 1) = \frac{1}{2}\right) =$$

$$V_N = \sum_{i=0}^{N-1} v_i = \# \text{ successes in } N$$

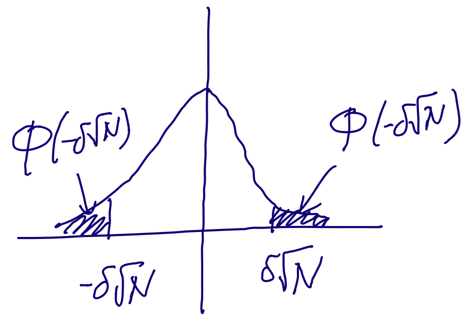
Bernoulli trials with

success probability $\frac{1}{2}$

use de Moivre-Laplace theorem.

$$= P_r\left(\frac{V_N - N/2}{\sqrt{N \cdot \frac{1}{2} \cdot \frac{1}{2}}} \geq \delta\sqrt{N} \,\Big/\, P_r(v_i = 1) = \frac{1}{2} \right) =$$

$$\frac{V_N - N/2}{\sqrt{N \cdot \frac{1}{2}\frac{1}{2}}} \to N(0,1) \quad \text{by de M-L th..}$$



$$\approx P_r\left(N(0,1) \geq \delta\sqrt{N} \right) =$$

$$= \Phi(-\delta\sqrt{N})$$

$$\alpha_N \leq \alpha \iff \Phi(-\delta\sqrt{N}) \leq \alpha \iff$$

t_α quantile of level α $\quad \Phi(t_\alpha) = \alpha$

$$\iff -\delta\sqrt{N} \leq t_\alpha \iff \boxed{N \geq \frac{t_\alpha^2}{\delta^2}}$$

Analyse

$$\beta_N = P_r\left(\text{accept as incorrect} \,/\, \text{correct} \right) =$$

$$= P_r\left(\frac{V_N}{N} < \frac{1}{2} + \delta/2 \,\Big/\, P_r(v_i = 1) = p = \frac{1}{2} + \delta \right) =$$

$$V_N = \sum_{i=0}^{N-1} v_i \quad \text{with success prob. } P_r(v_i = 1) = p.$$

$$= P_r\left(\frac{V_N - p \cdot N}{\sqrt{N \cdot p \cdot q}} < -\delta\sqrt{N} \,\Big/\, P_r(v_i = 1) = p = \frac{1}{2} + \delta \right)$$

By de Moivre-Laplace

$$\approx P_2\left(N(0,1) < -\delta\sqrt{N}\right) = \Phi(-\delta\sqrt{N})$$

$$\beta_N \leq \beta \iff \Phi(-\delta\sqrt{N}) \leq \beta \iff$$

$$-\delta\sqrt{N} \leq t_\beta \iff N \geq \frac{t_\beta^2}{\delta^2}.$$

Example. $\delta = \frac{1}{100}$

$$P_2(\varphi = F) \approx \frac{1}{2} - \frac{1}{100}$$

we want $\underbrace{\alpha_N, \beta_N \leq \frac{1}{8}}$

$$N \geq \frac{t_{\frac{1}{8}}^2}{\delta^2} = \frac{1.14^2}{\left(\frac{1}{100}\right)^2} \approx 13200$$

$$\Phi(t_{1/8}) = \frac{1}{8} \Rightarrow t_{1/8} \approx -1.14$$

if $\delta = \frac{1}{10} \Rightarrow N \geq 132$
