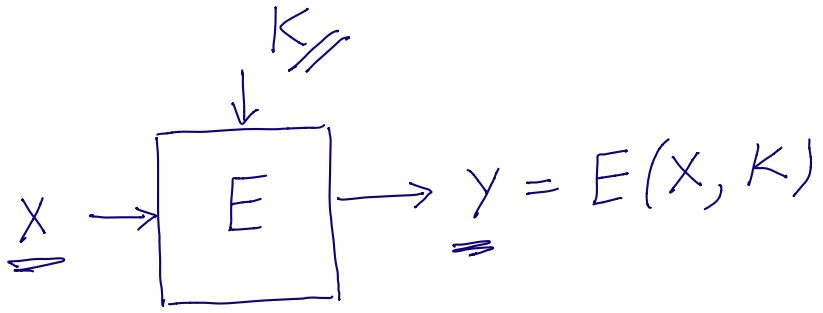
Linear Cryptanalysis.

Basic Approach.



AES-128 X, Y, K are 128-bit blocks.

known pl-text attack

given pl-text/c-text pairs
$X_i, Y_i \quad i = 1, \ldots, n$

recover K (or some bits of K)

Assumption $\underline{\Psi(X,Y)}$ and $\underline{\Phi(K)}$

correlation between Ψ and Φ s.t.

$$P_r(\Psi(X,Y) \oplus \Phi(K) = 0) = p \neq \frac{1}{2}$$

functions $\Psi(X,Y)$ and $\Phi(K)$ are recovered by analysing encryption function E.

Why linear cryptanalysis?

$\Psi(X,Y)$, $\Phi(K)$ are linear

commonly, ψ the correlation is ϕ

$$P_2\left(X[i_1]\oplus\cdots\oplus X[i_s]\oplus Y[j_1]\oplus\cdots\oplus Y[j_t]\oplus K[l_1]\oplus\cdots\oplus K[l_r]=0\right) = p \neq \frac{1}{2}$$

Basic Linear Cryptanalysis.

goal recover $\phi(K)$
effectively one key-bit.

1. count $n_0 = \#$ of $\psi(x_i, y_i) = 0$

2. decision rule

   2.1 $p > \frac{1}{2}$

   if $n_0 > n/2$ decide $\phi(K) = 0$

   $n_0 \leq n/2$ — " — $\phi(K) = 1$.

   2.2. $p < \frac{1}{2}$

   if $n_0 > n/2$ decide $\phi(K) = 1$

   $n_0 \leq n/2$ — " — $\phi(K) = 0$

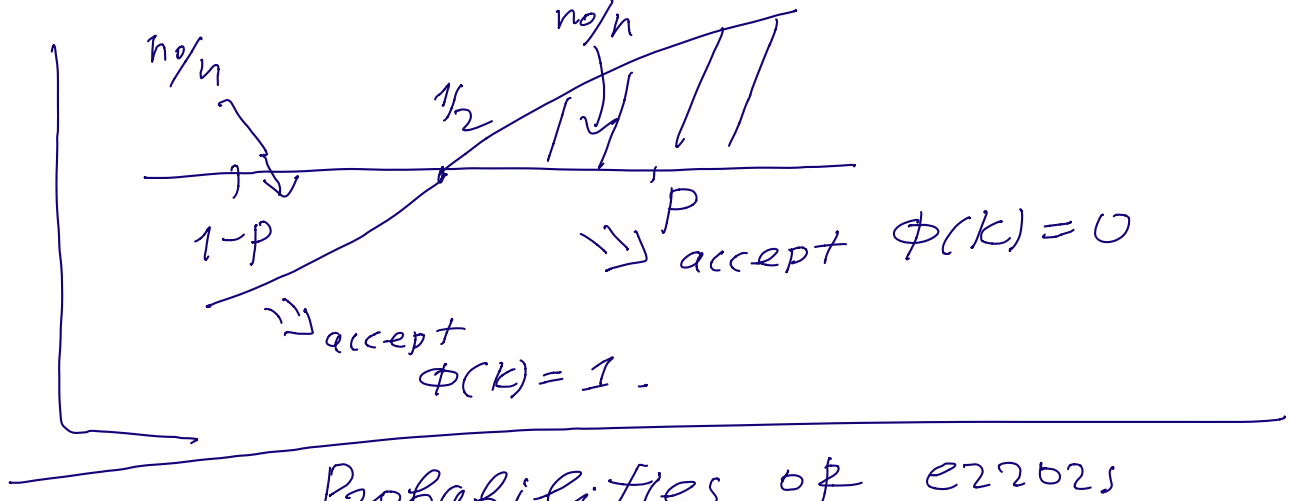
Comment why. assume $p > \frac{1}{2}$

and $\phi(K) = 0$

$\Rightarrow P_2(\psi(x,y) = 0) = p$

. $\phi(K) = 1$

$\Rightarrow P_2(\psi(x,y) = 0) = 1 - p$



Probabilities of errors

$\alpha = P_z$ (decide $\Phi(K)=0$ / correct $\Phi(K)=1$)

$\beta = P_z$ (decide $\Phi(K)=1$ / correct $\Phi(K)=0$)

Problem to solve:
How large $\underline{\underline{n}}$ to make α, β small?

Use de Moivre-Laplace theorem.

analyse α

assume $\Phi(K)=1 \Rightarrow$

$P_z(\psi(X,Y)=1) = p$

$P_z(\psi(X,Y)=0) = 1-p$

n_0 # successes in n Bernoulli trials with success probability $1-p$.

$p = \frac{1}{2} + \delta$, $\delta > 0$, small.

$$\alpha = P_2\left(n_0 > n/2 \;/\; \text{success prob.} = 1-p \right) =$$

$$= P_2\left(\frac{n_0 - (1-p)n}{\sqrt{np(1-p)}} > \frac{n/2 - (1-p)\cdot n}{\sqrt{np(1-p)}} \;/\; 1-p \right)$$

$\searrow$ tends to $N(0,1)$

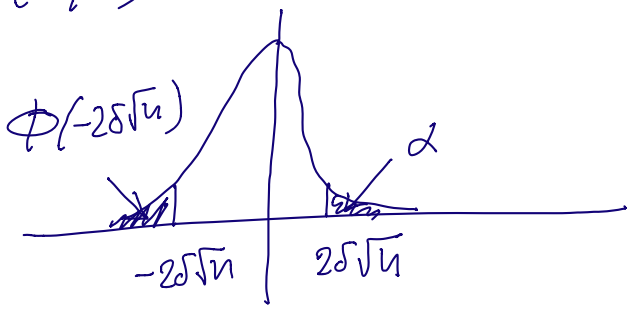
By de Moivre-Laplace TH.

$$\approx P_2\left(N(0,1) > 2\delta\sqrt{n} \right)$$

$p = \frac{1}{2} + \delta$, $p(1-p) = \frac{1}{4} - \delta^2 \approx \frac{1}{4}$ as δ small.

$$= \Phi\left(-2\delta\sqrt{n}\right)$$

$\Phi(x)$ $N(0,1)$ distribution function.



Now compute quantile t_2 s.t.

$$\Phi(t_2) = \alpha$$

$$-2\delta\sqrt{n} \approx t_2 \Rightarrow \boxed{n = \frac{t_2^2}{4\delta^2}}$$

Study

$$\beta = P_2(\text{decide } \Phi(K)=1 \,/\, \text{correct } \Phi(K)=0)$$

assume $\Phi(K)=0$

$$\Rightarrow \quad P_2(\Psi(X,Y)=0) = p$$
$$P_2(\Psi(X,Y)=1) = 1-p$$

n_0 # successes in n Bernoulli trials with success probability p ($\Psi(X,Y)=1$)

$$\beta = P_2\left(\underline{n_0 \le n/2} \,/\, \text{success prob. } p\right) =$$

$$= P_2\left(\frac{n_0 - pn}{\sqrt{n(1-p)\cdot p}} \le \frac{n/2 - pn}{\sqrt{n(1-p)\cdot p}} \,/\, p\right)$$

de Moivre-Laplace TH.

$$\approx P_2(N(0,1) \le -2\delta\sqrt{n})$$

$p = \frac{1}{2} + \delta$, $(1-p)p = \frac{1}{4} - \delta^2 \approx \frac{1}{4}$ small δ.

$$= \Phi(-2\delta\sqrt{n})$$

$\Rightarrow \quad \alpha \approx \beta$

$1-\alpha$ called success probability of this cryptanalysis.

Example. $\boxed{N = \frac{1}{\delta^2}}$

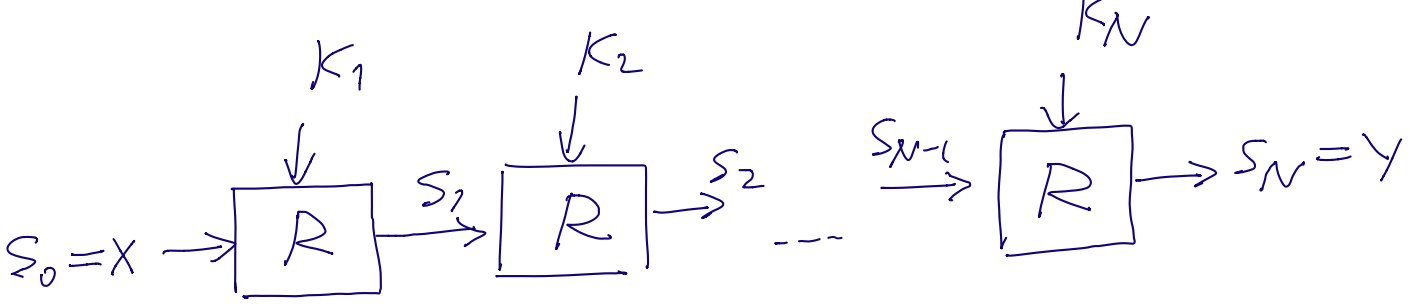
$$\alpha \approx \beta \approx \Phi\left(-2 \cdot \delta \sqrt{\frac{1}{\delta^2}}\right) = \Phi(-2) \approx 0{,}023$$

$\Rightarrow$ success prob.

$$1-\alpha \approx 0.977$$

How to find correlations for round block ciphers?

$$P_r\left(\underline{\psi(x,y)} \oplus \underline{\phi(k)} = 0\right) = \underline{p} \neq \frac{1}{2}$$



1. find correlation for each round.

$$P_r\left(\boxed{f_1 \cdot x \oplus g_1 \cdot s_1 \oplus h_1 \cdot k_1 = 0}\right) = \frac{1}{2} + \delta_1$$

input mask output mask key mask

$$P_2\left(f_2 \cdot S_1 \oplus g_2 \cdot S_2 \oplus R_2 \cdot K_2 = 0\right) = \frac{1}{2} + \delta_2$$

$$P_2\left(f_N \cdot S_{N-1} \oplus g_N \cdot Y \oplus R_N \cdot K_N = 0\right) = \frac{1}{2} + \delta_N$$

provide $f_{i+1} = g_i$, $i = 1, \dots, N-1$

$|\delta_i| \to \max$.

2. xor all correlations

$\Phi(x,y)$ $\quad$ $\Phi(k)$

$$P_2\left(f_1 \cdot X \oplus g_N \cdot Y \oplus R_1 \cdot K_1 \oplus \dots \oplus R_N K_N = 0\right) =$$

$$= \frac{1}{2} + 2^{N-1} \delta_1 \cdot \delta_2 \cdot \dots \cdot \delta_N .$$

apply this correlation in linear cryptanalysis and recover $\Phi(K)$.

Piling-up lemma

X_1, X_2 independent random variables s.t.

$$P_2(X_i = 0) = \frac{1}{2} + \delta_i$$

$$P_2(X_i = 1) = \frac{1}{2} - \delta_i$$

Then $P_2(X_1 \oplus X_2 = 0) = \frac{1}{2} + 2\cdot\delta_1\delta_2$

$P_2(X_1 \oplus X_2 = 1) = \frac{1}{2} - 2\cdot\delta_1\delta_2$.

Proof.

$P_2(X_1 \oplus X_2 = 0) = P_2(X_1 \oplus X_2 = 0, X_1 = 0) + P_2(X_1 \oplus X_2 = 0, X_1 = 1)$

complete probability formula.

$= P_2(X_2 = 0, X_1 = 0) + P_2(X_2 = 1, X_1 = 1)$

by independence

$= P_2(X_2 = 0)\cdot P_2(X_1 = 0) + P_2(X_2 = 1)\cdot P_2(X_1 = 1)$

$= \left(\frac{1}{2} + \delta_2\right)\left(\frac{1}{2} + \delta_1\right) + \left(\frac{1}{2} - \delta_2\right)\left(\frac{1}{2} - \delta_1\right)$

$= \frac{1}{2} + 2\delta_1\delta_2$ ▨

$X_1, \dots, X_N$ s.t. $P_2(X_i = 0) = \frac{1}{2} + \delta_i$

$P_2(X_i = 1) = \frac{1}{2} - \delta_i$

independent

$P_2(X_1 \oplus X_2 \oplus \dots \oplus X_N = 0) = \frac{1}{2} + 2^{N-1}\cdot\delta_1\cdot\delta_2\cdots\delta_N$

by iterating Piling-up lemma.