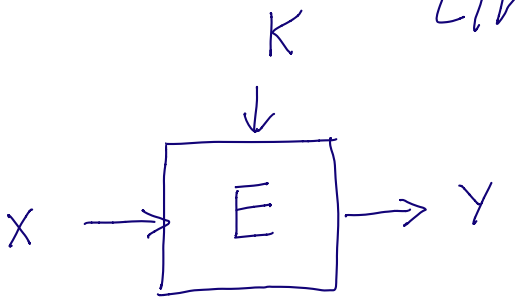
Continue with Linear Cryptanalysis



$$Pr\left(\psi(X,Y) \oplus \Phi(K) = 0\right) = \frac{1}{2} + \delta, \quad \delta \neq 0$$

Boolean, linear

known pl.-text attack.

$x_i, y_i \quad i = 1 \ldots n$

pl.-text/c.-text pairs.

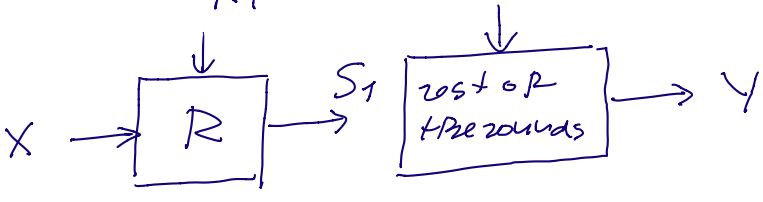
Goal recover some bits of the key K.

find $\Phi(K) \Leftrightarrow$ 1 bit of K.

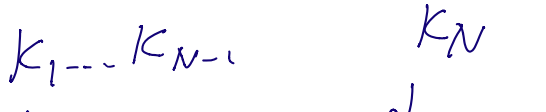
Improvents on Linear Cryptanalysis.

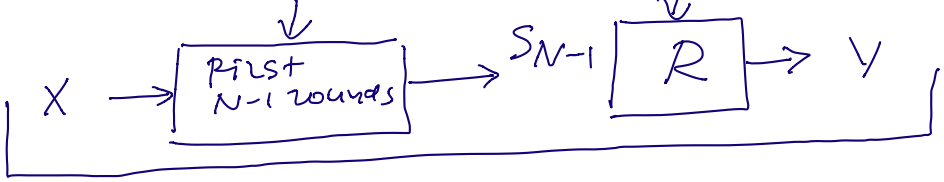
split encryption into 2 parts

first and the rest



last round and the rest.





assume correlation

$$P_r\left(\Psi(X, S_{N-1}) \oplus \varphi(K) = 0\right) = \frac{1}{2} + \delta_1, \quad \delta_1 \neq 0$$

based on $N-1$ round encryption,

$|\delta_1| > |\delta|$ (based on N round-encryption)

goal find $\varphi(K)$ and K_N (last round key)

Algorithm

1. for each value of $K_N = k$

count

$$n_0(k) = \#\ \Psi(X_i, S_{N-1}) = 0$$
$$S_{N-1} = R^{-1}(y_i, k)$$
$$i = 1, \ldots, n$$

2. decision

decide $K_N = k$ if $\left| n_0(k) - \frac{n}{2} \right| \to \max.$

3. assume $\delta_1 > 0$

decide $\varphi(K) = \begin{cases} 0 & n_0 \geq n/2 \\ 1 & n_0 < n/2. \end{cases}$

output $\varphi(K)$, K_N.

How large n to make this work.

[We know if $n > 8/\delta_1^2$ then
success prob. > 0.9

complexity $2^{|K_N|} \cdot n$ very large.

Another improvements

work block cipher constructed with R
small S-boxes $S: \ell\text{-bit} \to \ell\text{-bit}$
in SPN, ℓ small. (in AES $\ell = 8$)
SPN $\ell = 4$

Correlation

$$P_r\left(\psi(\bar{x}, \bar{s}_{N-1}) \oplus \phi(K) = 0\right) = \frac{1}{2} + \delta_1$$

$$\bar{s}_{N-1} = R^{-1}(\bar{y}, \bar{K}_N)$$

$\bar{x}$	substring of	x
$\bar{y}$	—"—	y
$\bar{s}_{N-1}$	—"—	s_{N-1}
$\bar{K}_N$	—"—	K_N

Algorithm

2. For any value of $\overline{K_N} = k$

$$n_0(k) = \#\ \psi(\overline{x_i}, \overline{s_{N-1}}) = 0$$

$$\overline{s_{N-1}} = \hat{R}^{-1}(\overline{y_i}, k)$$

$$i = 1, \dots, n$$

2. decide $\overline{K_N} = k$

$$|n_0(k) - n/2| \to \max$$

$$\phi(k) = \begin{cases} 0 & n_0(k) \geq n/2 \\ 1 & < \end{cases}$$

$(\delta_1 > 0)$

$n > 8/\delta_1^2$ For success prob. > 0.9

complexity

using 2 counters, $|\overline{x}|+|\overline{y}|$

address a, b ($|\overline{x}|$ - strings of bits, $|\overline{y}|$ - strings of bits)

$$v_{a,b} = \#\ \overline{x_i}, \overline{y_i} = a, b \quad i = 1, \dots n.$$

$$\Rightarrow \boxed{n_0(k) = \sum_{a,b} f(a,b,k) \cdot v_{a,b}}$$

$$f(a,b,k) = \begin{cases} 1 & \psi(a, \overline{s_{N-1}}) = 0 \\ & \overline{s_{N-1}} = \hat{R}^{-1}(b,k) \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{complexity} = n + 2^{|\bar{x}|+|\bar{y}|+|K_N|}$$

use that round key is xored with R state

another formula for $n_0(k) =$

$$\sum_{a,b} f(a, b \oplus k) v_{a,b}$$

a, b ; b, k.

convolution of two real-valued functions.

may be efficiently computed with Walsh-Hadamard transform.

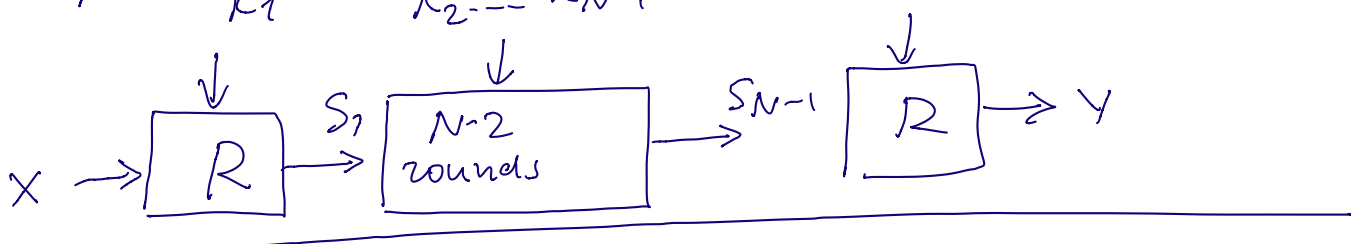
$$|\bar{x}|+|\bar{y}|$$

$$\Rightarrow \quad n + 3 \cdot |K_N| \cdot 2$$

complexity.

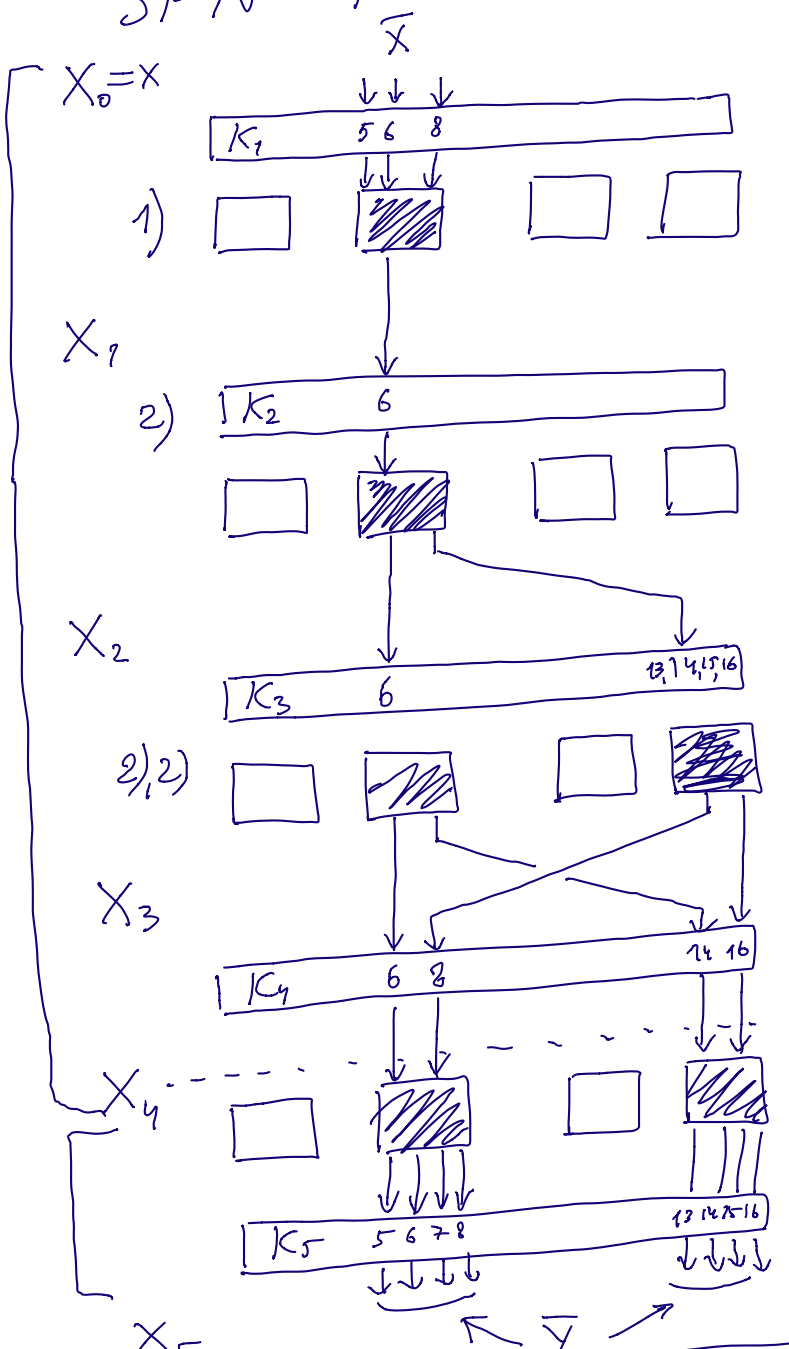
Further improvements.

split encryption into 3 parts



Example.

Apply Linear Cryptanalysis to SPN from Stinson's book.



active S-boxes $\bar{X}, \bar{Y}$, $\bar{K}_5 = K_5[5,6,7,8, 13,14,15,16]$

define $\Phi(K)$

round 1

$X_0\{5,6,8\} \oplus K_1\{5,6,8\} \oplus X_1\{6\} = 0$ $\quad \frac{1}{2} + \frac{1}{4}$

round 2

$X_1\{6\} \oplus K_2\{6\} \oplus X_2\{6,14\} = 0$ $\quad \frac{1}{2} - \frac{1}{4}$

round 3

$X_2\{6\} \oplus K_3\{6\} \oplus X_3\{6,14\} = 0$ $\quad \frac{1}{2} - \frac{1}{4}$

$X_2\{14\} \oplus K_3\{14\} \oplus X_3\{8,16\} = 0$ $\quad \frac{1}{2} - \frac{1}{4}$

$X_3\{6,8,14,16\} = X_4\{6,8,14,16\} \oplus K_4\{6,8,14,16\}$

xor all expressions

after cancellation

$X_0\{5,6,8\} \oplus X_4\{6,8,14,16\} \oplus k = 0$ with

prob. $\frac{1}{2} + 2^3 \cdot \frac{1}{4} \cdot \left(-\frac{1}{4}\right)^3 = \frac{1}{2} - \frac{1}{32}$

$k = K_1\{5,6,8\} \oplus \dots \oplus K_4\{6,8,14,16\}$

analysis of the SPN S-box

$S[\overbrace{X_1 X_2 X_3 X_4}^{X}] = \overbrace{Y_1 Y_2 Y_3 Y_4}^{Y}$

use only two correlation for the S-box

$Pr(X\{1,2,4\} \oplus Y\{2\} = 0) = \frac{3}{4} = \frac{1}{2} + \frac{1}{4}$ 1)

$X[1] \oplus X[2] \oplus X[4] \quad Y[2]$

$x_1 \quad x_2 \quad x_4 \quad y_2$

$$\Pr\left(X\{2\} \oplus Y\{2,4\} = 0\right) = \frac{1}{4} = \frac{1}{2} - \frac{1}{4}. \quad 2)$$

$X\{2\} = X[2] = x_2$

$Y\{2,4\} = Y[2] \oplus Y[4] = y_2 \oplus y_4$

Apply algorithm 9 recover key-bits

$\overbrace{K_5}^{8\text{-bit}}, \overbrace{k}^{1\text{-bit}}$.

How large n to get high success prob.

$$n \gg \frac{8}{\delta_1^2} = \frac{8}{\left(-\frac{1}{32}\right)^2} = 2^{13} \approx \boxed{8000}$$

$\delta_1 = -\frac{1}{32}$
