# LINEAR CRYPTANALYSIS

Halil İbrahim Kaplan

Middle East Technical University

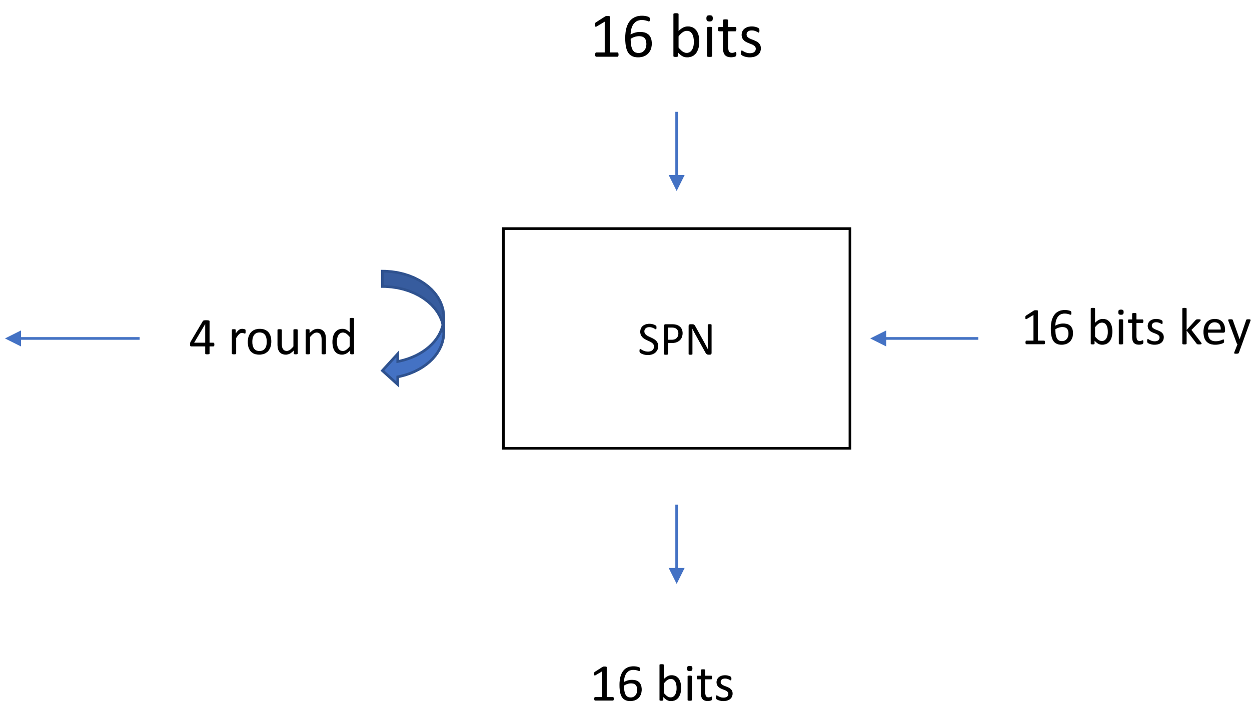
April 5 , 2021

# Overview

- SPN
- Constructing Linear Approximation
- Extracting Key Bits
- Attack Simulation
- Complexity of Attack

# SPN

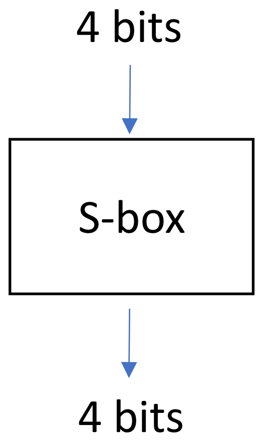
1) Key addition
2) Substiution
3) Permutation



# SPN

**SUBSTITUTION:**

- We divide 16 bit data block into 4 bit sub blocks.
- S- boxes are bijective.
- $S(a \oplus b) \neq S(a) \oplus S(b)$




| input | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| output | E | 4 | D | 1 | 2 | F | B | 8 | 3 | A | 6 | C | 5 | 9 | 0 | 7 |

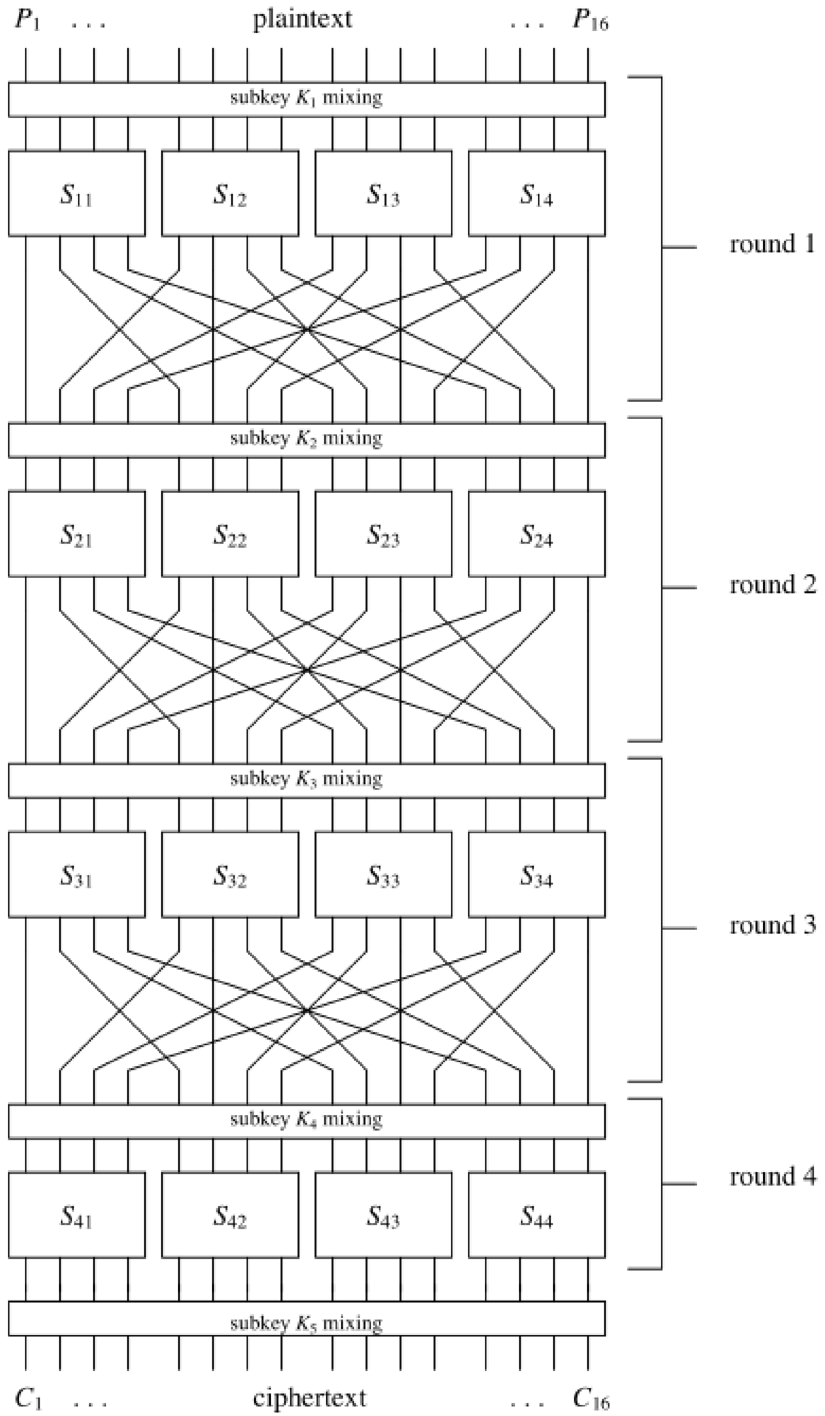
**Table 1.** S-box Representation (in hexadecimal)

## PERMUTATION :

- It is simply permutation of the bit pozitions.
- Last round does not have permutation.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| input | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| output | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 | 15 | 4 | 8 | 12 | 16 |

**Table 2.** Permutation



$P_1$ . . . plaintext . . . $P_{16}$
subkey $K_1$ mixing
$S_{11}$
$S_{12}$
$S_{13}$
$S_{14}$
round 1
subkey $K_2$ mixing
$S_{21}$
$S_{22}$
$S_{23}$
$S_{24}$
round 2
subkey $K_3$ mixing
$S_{31}$
$S_{32}$
$S_{33}$
$S_{34}$
round 3
subkey $K_4$ mixing
$S_{41}$
$S_{42}$
$S_{43}$
$S_{44}$
round 4
subkey $K_5$ mixing
$C_1$ . . . ciphertext . . . $C_{16}$

# Constructing Linear Approximation

- The approach in linear cryptanalysis is to determine expression like below which have high or low probablty of occurrence.

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0 \qquad (1)$$

where $X_i$ represents the $i$-th bit of the input $X = [X_1, X_2, \ldots]$ and $Y_j$ represents the $j$-th bit of the output $Y = [Y_1, Y_2, \ldots]$. This equation is representing the exclusive-OR "sum" of $u$ input bits and $v$ output bits.

# Constructing Linear Approximation

*Piling-Up Lemma* (Matsui [1])

For $n$ independent, random binary variables, $X_1, X_2, \ldots X_n$,

$$\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

or, equivalently,

$$\varepsilon_{1,2,\ldots,n} = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

where $\varepsilon_{1,2,\ldots,n}$ represents the bias of $X_1 \oplus \ldots \oplus X_n = 0$.

# Constructing Linear Approximation

$let$

For $X_1 = \varepsilon_1 = 1/4$
For $X_2 = \varepsilon_2 = 1/4$
For $X_3 = \varepsilon_3 = 1/4$

Then by Piling-up lemma

$\varepsilon_{1,3}$ = 2*(1/4*1/4)=1/8

But we know that

$X_1 \oplus X_3$=($X_1 \oplus X_2$) $\oplus$($X_2 \oplus X_3$)

If $X_1 \oplus X_2$ and $X_2 \oplus X_3$ are independent by Piling-up lemma

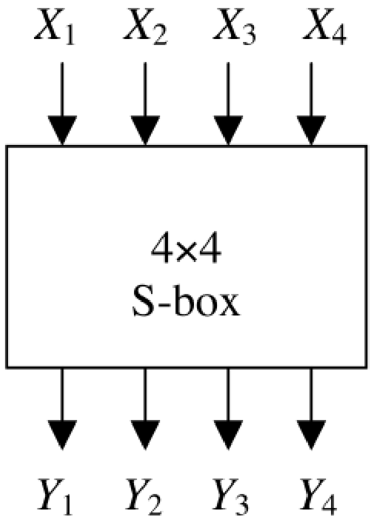
$\varepsilon_{1,3}$ = 2*(1/8*1/8)=1/32 $\neq$ 1/8

So $X_1 \oplus X_2$ and $X_2 \oplus X_3$ are **not** independent

# Constructing Linear Approximation

| $X_1$ | $X_2$ | $X_3$ | $X_4$ | $Y_1$ | $Y_2$ | $Y_3$ | $Y_4$ | $X_2 \oplus X_3$ | $Y_1 \oplus Y_3 \oplus Y_4$ | $X_1 \oplus X_4$ | $Y_2$ | $X_3 \oplus X_4$ | $Y_1 \oplus Y_4$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |

$\frac{12}{16}$ $\frac{8}{16}$ $\frac{2}{16}$



# Constructing Linear Approximation

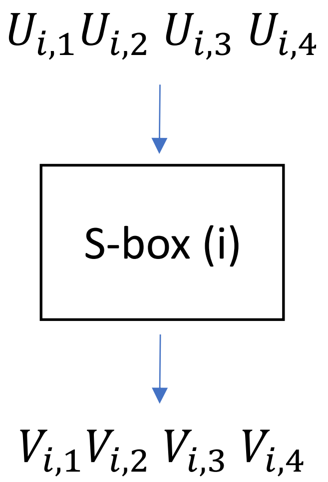
(Matches – 8)

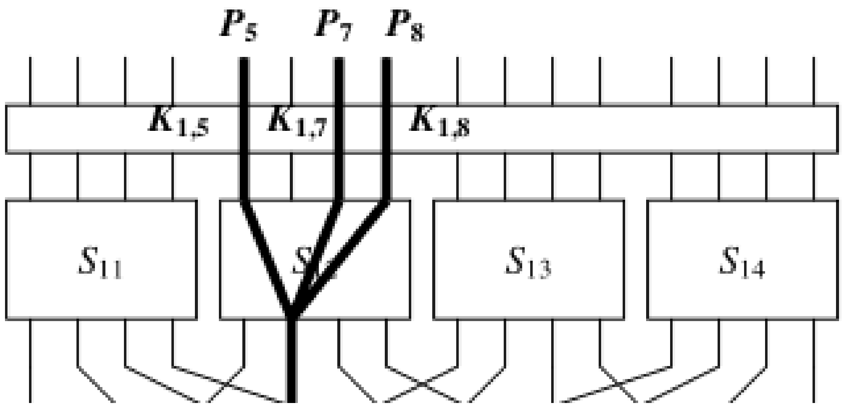
| Input Sum \ Output Sum | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | +8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | −2 | −2 | 0 | 0 | −2 | +6 | +2 | +2 | 0 | 0 | +2 | +2 | 0 | 0 |
| 2 | 0 | 0 | −2 | −2 | 0 | 0 | −2 | −2 | 0 | 0 | +2 | +2 | 0 | 0 | −6 | +2 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | +2 | −6 | −2 | −2 | +2 | +2 | −2 | −2 |
| 4 | 0 | +2 | 0 | −2 | −2 | −4 | −2 | 0 | 0 | −2 | 0 | +2 | +2 | −4 | +2 | 0 |
| 5 | 0 | −2 | −2 | 0 | −2 | 0 | +4 | +2 | −2 | 0 | −4 | +2 | 0 | −2 | −2 | 0 |
| 6 | 0 | +2 | −2 | +4 | +2 | 0 | 0 | +2 | 0 | −2 | +2 | +4 | −2 | 0 | 0 | −2 |
| 7 | 0 | −2 | 0 | +2 | +2 | −4 | +2 | 0 | −2 | 0 | +2 | 0 | +4 | +2 | 0 | +2 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | −2 | +2 | +2 | −2 | +2 | −2 | −2 | −6 |
| 9 | 0 | 0 | −2 | −2 | 0 | 0 | −2 | −2 | −4 | 0 | −2 | +2 | 0 | +4 | +2 | −2 |
| A | 0 | +4 | −2 | +2 | −4 | 0 | +2 | −2 | +2 | +2 | 0 | 0 | +2 | +2 | 0 | 0 |
| B | 0 | +4 | 0 | −4 | +4 | 0 | +4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| C | 0 | −2 | +4 | −2 | −2 | 0 | +2 | 0 | +2 | 0 | +2 | +4 | 0 | +2 | 0 | −2 |
| D | 0 | +2 | +2 | 0 | −2 | +4 | 0 | +2 | −4 | −2 | +2 | 0 | +2 | 0 | 0 | +2 |
| E | 0 | +2 | +2 | 0 | −2 | −4 | 0 | +2 | −2 | 0 | 0 | −2 | −4 | +2 | −2 | 0 |
| F | 0 | −2 | −4 | −2 | −2 | 0 | +2 | 0 | 0 | −2 | +4 | −2 | −2 | 0 | +2 | 0 |

**Table 4.** Linear Approximation Table

# Constructing Linear Approximation

$S_{12}$: $X_1 \oplus X_3 \oplus X_4 = Y_2$ with probability 12/16 and bias +1/4
$S_{22}$: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias –1/4
$S_{32}$: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias –1/4
$S_{34}$: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias –1/4



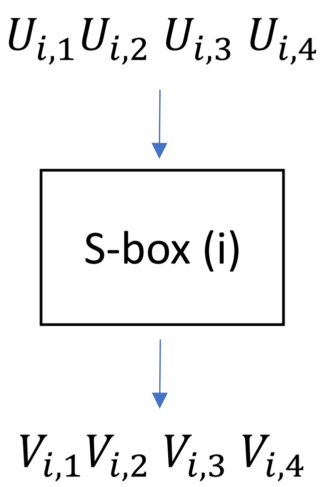



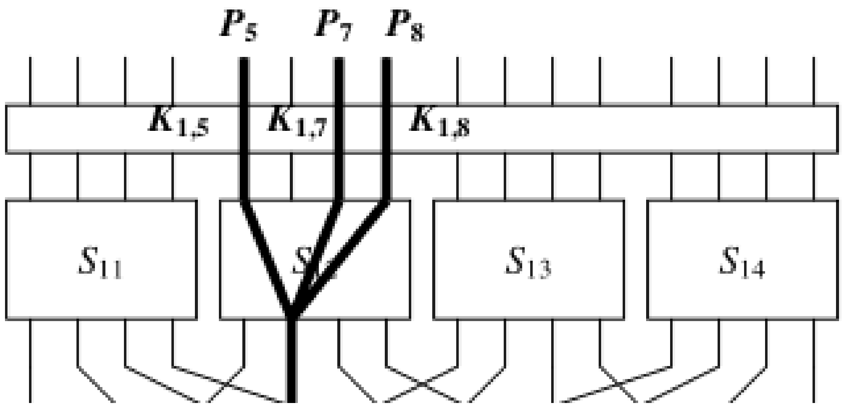

$$\begin{aligned} V_{1,6} &= U_{1,5} \oplus U_{1,7} \oplus U_{1,8} \\ &= (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8}) \end{aligned}$$

Probablity= 3/4

# Constructing Linear Approximation

$S_{12}: X_1 \oplus X_3 \oplus X_4 = Y_2$ with probability 12/16 and bias +1/4



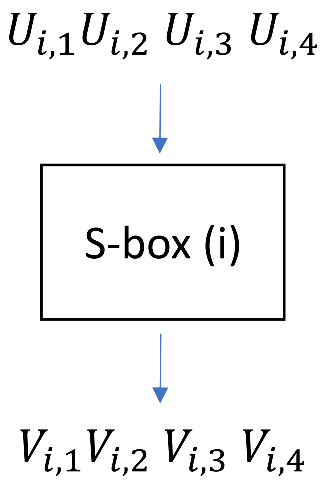



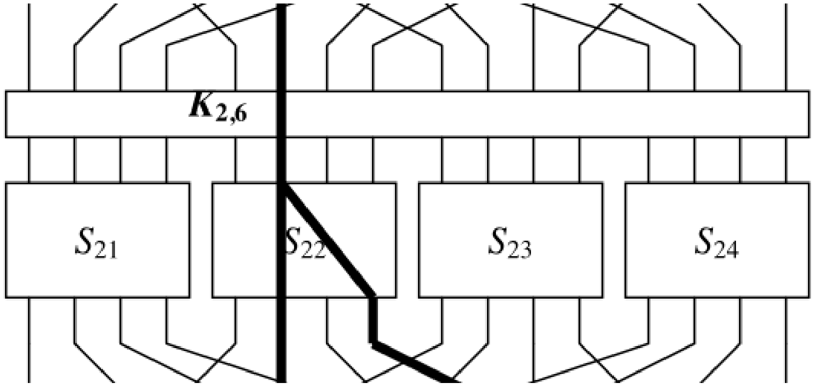

$$
\begin{aligned}
V_{1,6} &= U_{1,5} \oplus U_{1,7} \oplus U_{1,8} \\
&= (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8})
\end{aligned}
$$

Probablity= 3/4

# Constructing Linear Approximation

$S_{22}$: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias −1/4




$$V_{2,6} \oplus V_{2,8} = U_{2,6}$$

with probability 1/4. Since $U_{2,6} = V_{1,6} \oplus K_{2,6}$, we can get an approximation of the form

$$V_{2,6} \oplus V_{2,8} = V_{1,6} \oplus K_{2,6}$$

# Constructing Linear Approximation

$$V_{1,6} = (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8})$$

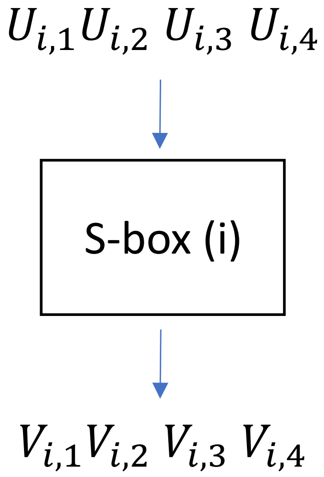
$$\oplus \quad V_{2,6} \oplus V_{2,8} = V_{1,6} \oplus K_{2,6}$$

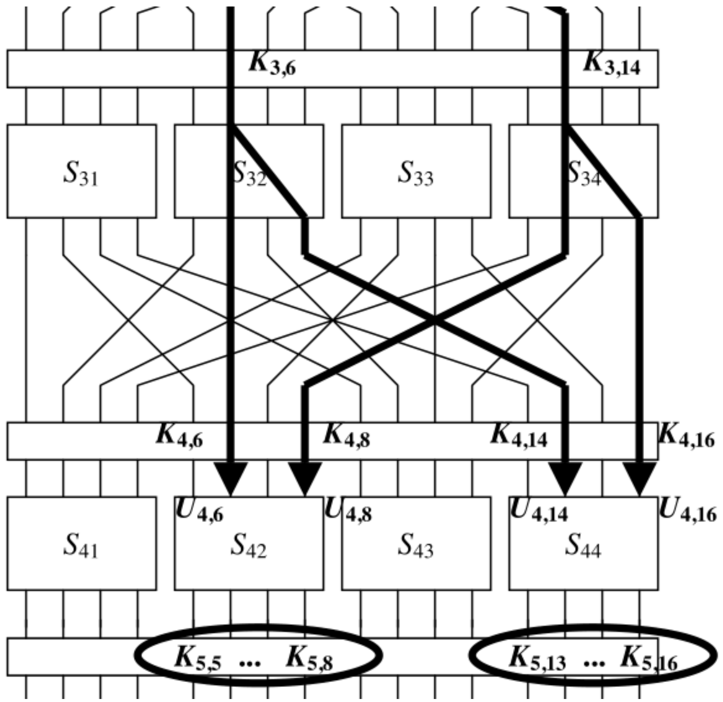
$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} = 0 \qquad (3)$$

**Holds with probabity =** ½+2(3/4-1/2)(1/4-1/2) =1/32

# Constructing Linear Approximation

$S_{32}$: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias −1/4
$S_{34}$: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias −1/4




For round 3, we note that

$$V_{3,6} \oplus V_{3,8} = U_{3,6}$$

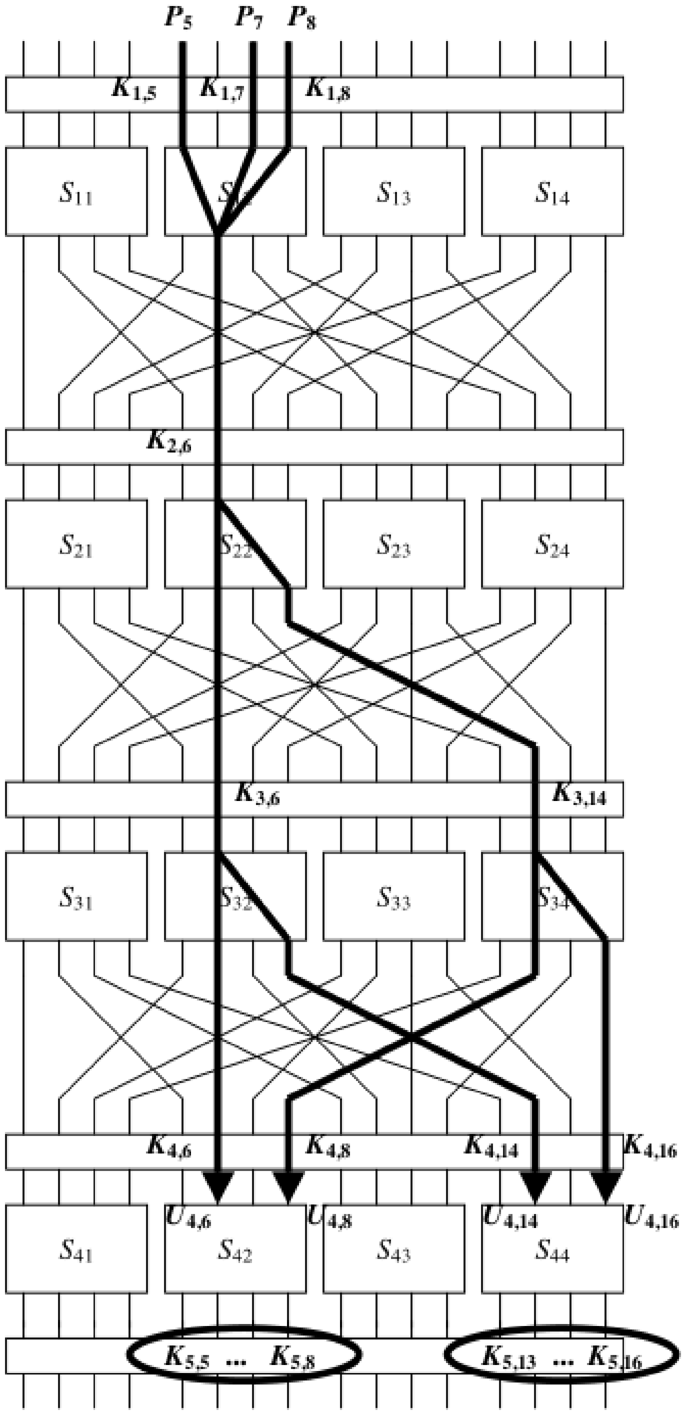
with probability 1/4 and

$$V_{3,14} \oplus V_{3,16} = U_{3,14}$$

with probability 1/4. Hence, since $U_{3,6} = V_{2,6} \oplus K_{3,6}$ and $U_{3,14} = V_{2,8} \oplus K_{3,14}$,

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} = 0 \qquad (4)$$

with probability of $1/2 + 2(1/4-1/2)^2 = 5/8$ (that is, with a bias of +1/8). Again, we have applied the Piling-Up Lemma.



P5 P7 P8
K1,5 K1,7 K1,8
S11 S12 S13 S14
K2,6
S21 S22 S23 S24
K3,6 K3,14
S31 S32 S33 S34
K4,6 K4,8 K4,14 K4,16
U4,6 U4,8 U4,14 U4,16
S41 S42 S43 S44
K5,5 ... K5,8
K5,13 ... K5,16

# Constructing Linear Approximation

Now combining (3) and (4), to incorporate all four S-box approximations, we get

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus P_5 \oplus P_7 \oplus P_8 \\ \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} = 0.$$

Noting that $U_{4,6} = V_{3,6} \oplus K_{4,6}$, $U_{4,8} = V_{3,14} \oplus K_{4,8}$, $U_{4,14} = V_{3,8} \oplus K_{4,14}$, and $U_{4,16} = V_{3,16} \oplus K_{4,16}$, we can then write

$$\boxed{U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0.} \qquad (5)$$

where

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}$$

# Constructing Linear Approximation

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0.$$

If

$$\boldsymbol{\Sigma_K = 0}$$

By Piling – Up lemma, above expression holds with probablity

$$P = \frac{1}{2} + 2^3\left(\frac{3}{4} - \frac{1}{2}\right)\left(\frac{1}{4} - \frac{1}{2}\right)^3 = \frac{15}{32},\ Bias = \frac{16}{32} - \frac{15}{32} = \frac{1}{32}$$

If

$$\boldsymbol{\Sigma_K = 1}$$

$$P = 1 - \frac{15}{32} = \frac{17}{32},\ Bias = \frac{16}{32} - \frac{17}{32} = -\frac{1}{32}$$

# Extracting Key Bits

Ciphertext bits

$\oplus$

Key candidate

$$S^{-1}$$

Check if the linear equation satisfied

If yes, increase count for the key candidate

Will be done for all known Plaintext/Ciphertext couples

Will be done for all possible key candidate

# Extracting Key Bits

Ciphertext bits

$\oplus$

Key candidate

↓

$\boxed{S^{-1}}$

↓

Check if

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0$$

Satisfied for key candidate

↓

If yes, increase count for the key candidate

Will be done for 10.000 Plaintext/Ciphertext couples

Will be done for $2^8$ Possible key candidate

# Attack Simulation

- $[K_{5,5} \ldots K_{5,8}]$=[0010] (hex 2 )and $[K_{5,13} \ldots K_{5,16}]$=[0100] (hex 4 ) determined before Attack.
- |bias|=|count-5000|/10.000

$\boldsymbol{Expected\ Bias} = \frac{1}{32}$**=0.03125**

| *partial subkey* $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$ | \| bias \| | *partial subkey* $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$ | \| bias \| |
|---|---|---|---|
| 1 C | 0.0031 | 2 A | 0.0044 |
| 1 D | 0.0078 | 2 B | 0.0186 |
| 1 E | 0.0071 | 2 C | 0.0094 |
| 1 F | 0.0170 | 2 D | 0.0053 |
| 2 0 | 0.0025 | 2 E | 0.0062 |
| 2 1 | 0.0220 | 2 F | 0.0133 |
| 2 2 | 0.0211 | 3 0 | 0.0027 |
| 2 3 | 0.0064 | 3 1 | 0.0050 |
| **2 4** | **0.0336** | 3 2 | 0.0075 |
| 2 5 | 0.0106 | 3 3 | 0.0162 |
| 2 6 | 0.0096 | 3 4 | 0.0218 |
| 2 7 | 0.0074 | 3 5 | 0.0052 |
| 2 8 | 0.0224 | 3 6 | 0.0056 |
| 2 9 | 0.0054 | 3 7 | 0.0048 |

# Complexity of Attack

- Number of required known plaintext $= N_L \approx \frac{1}{\varepsilon^2}$

  for linear cryptanlaysis.

$$= \frac{1}{(\frac{1}{32})^2}$$

$$= 1024$$

Number of S – box used in Linear Approximtion increase $\Rightarrow$ Bias increase $\Rightarrow$ Number of required known plaintext increase

# References

[1] Heys, H. (2001). ”A tutorial on linear and differential cryptanalysis.”
Waterloo, Ont.: Faculty of Mathematics, University of Waterloo.

[2] Matsui, M. (1993), “Linear Cryptanalysis Method for DES Cipher.”
EUROCRYPT’93