DIFFERENTIAL CRYPTANALYSIS

Halil İbrahim Kaplan

2021

TÜBİTAK
BİLGEM

Overview

- Analyzing the Attack
- Constructing Differential Characteristics
- Extracting Key Bits
- Complexity of Attack

Analyzing the Attack

- Differential Cryptanalysis exploits the high probability of certain occurrences of plaintext differences ΔX and differences into the last round of the cipher ΔY.

- In an ideally randomizing cipher :

  For particular ΔX , probability that particular ΔY occurs $= 1/2^n$

  (where n is the number of bits of X.)

- Differential cryptanalysis seeks :

  For particular ΔX , probability that particular ΔY occurs $>> 1/2^n$

  (where n is the number of bits of X.)

Analyzing the Attack

- Differential cryptanalysis is a chosen plaintext attack.
- Attacker will select X *and* X' so that $\Delta X = X \oplus X'$
- Corresponding ΔY will occure with high probability

Analyzing the Attack

- We want to construct differential $(\Delta X, \Delta Y)$

Plaintext Difference

Difference of the input to the last round

We shall do this by examining high likely **differential characteristic**

Constructing Differential Characteristics

Differential characteristic :

Sequence of input and output differences to the rounds so that the output difference from one round corresponds to the input difference for the next round.

	Probability
$(\Delta X, \Delta Y_1)$	P_1
$(\Delta Y_1, \Delta Y_2)$	P_2
$(\Delta Y_2, \Delta Y)$	P_3
$(\Delta X, \Delta Y)$	$P_1 \times P_2 \times P_3$

Constructing Differential Characteristics

With probability $\frac{8}{16}$, $\Delta Y = 0010$ will occur for arbitrary pair satisfying $\Delta X = 1011$ (In ideal S-box probability expected: $\frac{1}{16}$)

X	Y	ΔY		
		$\Delta X = 1011$	$\Delta X = 1000$	$\Delta X = 0100$
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

Table 6. Sample Difference Pairs of the S-box

Constructing Differential Characteristics

ΔY *values*

ΔX *values*

Input Difference	Output Difference 0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Table 7. Difference Distribution Table

Constructing Differential Characteristics

Some properties of the difference distribution table:

1) Sum of all elements in a row is 2^n = 16

2) All element values are even.

3) If we could construct an ideal S-box, all elements in the table equal to 1 and the probability of occurrence of a particular value for ΔY given a particular value of ΔX would be 1/ 2^n = 1/16.

Constructing Differential Characteristics

Influence of the key on s-box differential :

Input of unkeyed S-box = X_i

Input of keyed S-box = W_i

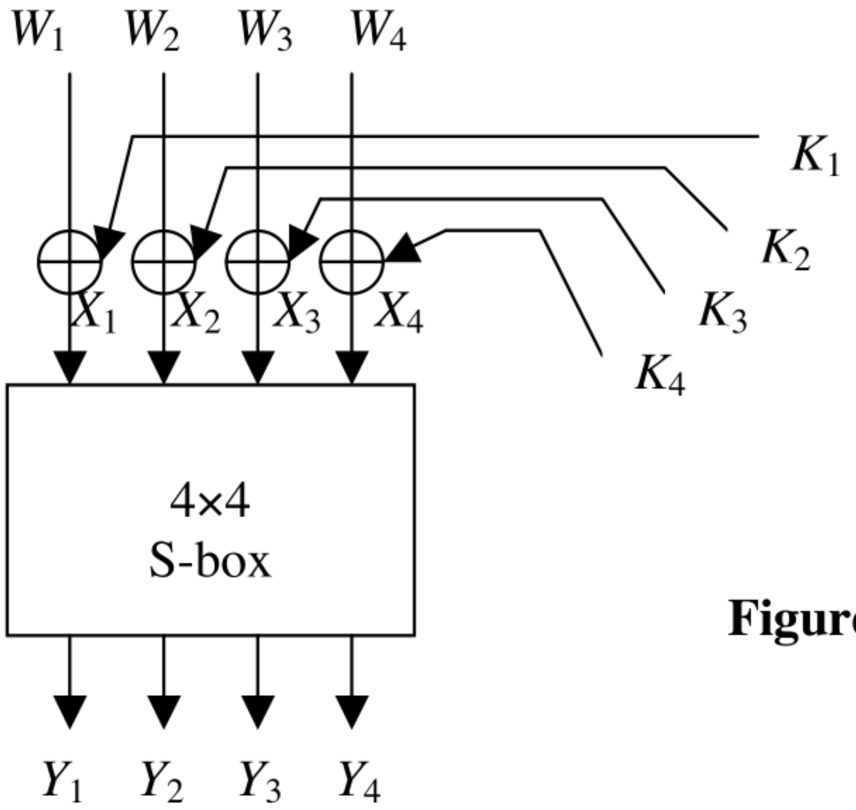


Figure 4. Keyed S-box

$$\Delta W_i = W_i' \oplus W_i'' = (X_i' \oplus K_i) \oplus (X_i'' \oplus K_i) = X_i' \oplus X_i'' = \Delta X_i$$

Constructing Differential Characteristics

To determine useful differential characteristic of overall cipher , we will concatenate appropriate difference pairs of S-boxes.

We use the following difference pairs of the S-box:

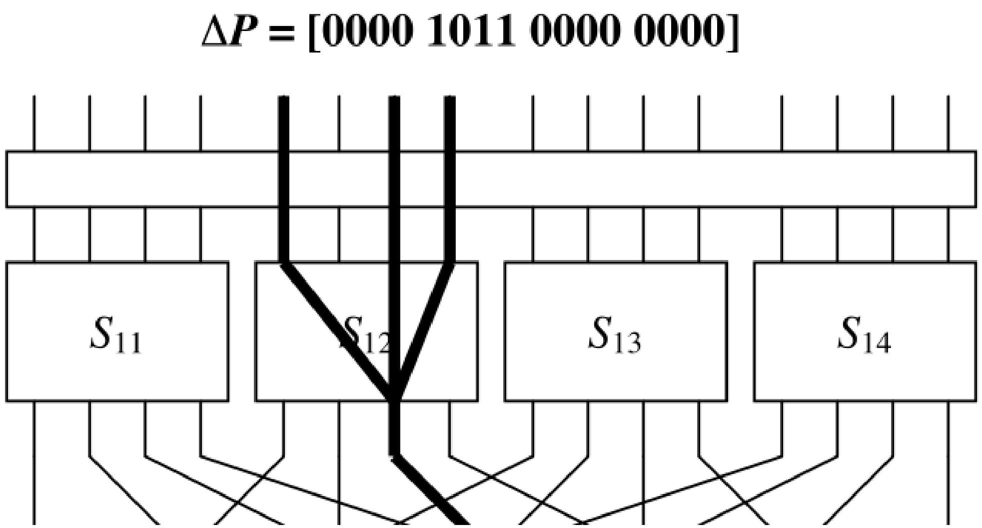
S_{12}: $\Delta X = \mathrm{B} \rightarrow \Delta Y = 2$ with probability 8/16
S_{23}: $\Delta X = 4 \rightarrow \Delta Y = 6$ with probability 6/16
S_{32}: $\Delta X = 2 \rightarrow \Delta Y = 5$ with probability 6/16
S_{33}: $\Delta X = 2 \rightarrow \Delta Y = 5$ with probability 6/16

All other S-boxes will have zero input difference and consequently zero output difference.

The input difference to the cipher is equivalent to the input difference to the first round and is given by

$$\Delta P = \Delta U_1 = [0000\ 1011\ 0000\ 0000]$$

Constructing Differential Characteristics



$$With\ probability\ \frac{8}{16} = \frac{1}{2}$$

$$\Delta P = \Delta U_1 = [0000\ 1011\ 0000\ 0000]$$

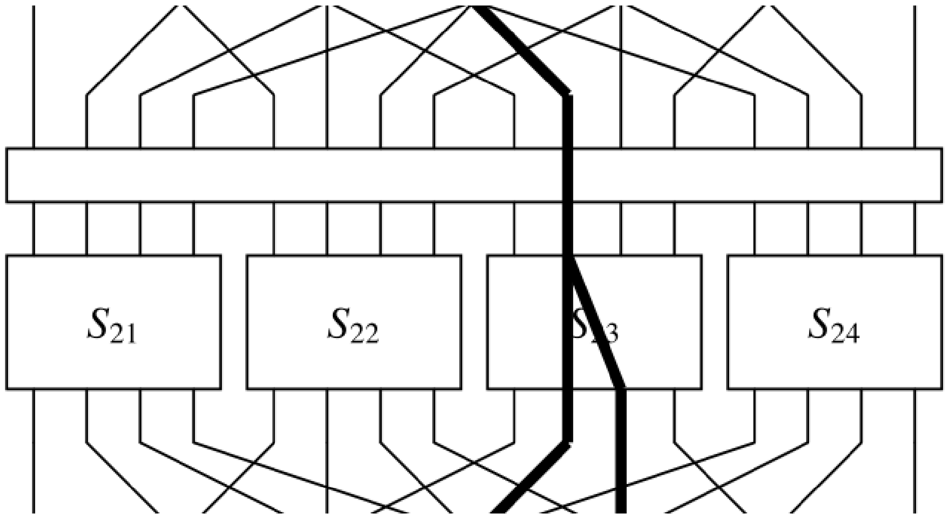
$$\downarrow S - box$$

$$\Delta V_1 = [0000\ 0010\ 0000\ 0000]$$

$$\downarrow Permutation$$

$$\Delta U_2 = [0000\ 0000\ 0100\ 0000]$$

Constructing Differential Characteristics



$$\Delta U_2 = [0000\ 0000\ 0100\ 0000]$$

$$\xrightarrow{S-box}$$

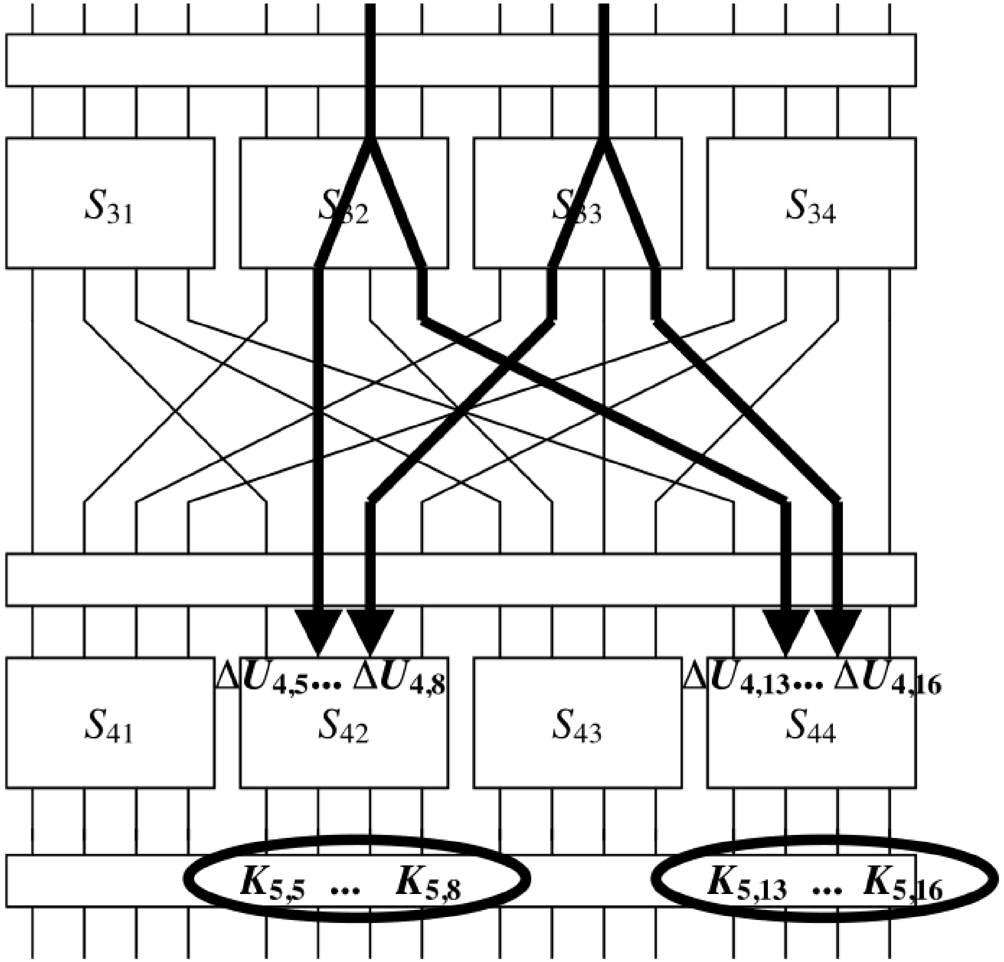
$$\Delta V_2 = [0000\ 0000\ 0110\ 0000]$$

$$\xrightarrow{Permutation}$$

$$\Delta U_3 = [0000\ 0010\ 0010\ 0000]$$

$$With\ probability\ \frac{6}{16} = \frac{3}{8}$$

Constructing Differential Characteristics



$$With\ probability\ \frac{6}{16} x \frac{6}{16} = \frac{9}{64}$$

$$\Delta U_3 = [0000\ 0010\ 0010\ 0000]$$

$$\downarrow S - boxes$$

$$\Delta V_3 = [0000\ 0101\ 0101\ 0000]$$

$$\downarrow Permutation$$

$$\Delta U_4 = [0000\ 0110\ 0000\ 0110]$$

Constructing Differential Characteristics

$$With\ independance\ assumption, total\ probability = \frac{6}{16} x \frac{6}{16} x \frac{6}{16} x \frac{8}{16} = \frac{27}{1024}$$

During the cryptanalysis process, many pairs of plaintexts for which Δ P = [0000 1011 0000 0000] will be encrypted.

With high probability, 27/1024, the differential characteristic illustrated will occur.

We term such pairs for Δ P as right pairs.

Plaintext difference pairs for which the characteristic does not occur are referred to as wrong pairs.

Extracting Key Bits

Ciphertexts

$\bigoplus$

Key candidate

↓

S^{-1}

↓

Check if

$\Delta U_4 = [0000\ 0110\ 0000\ 0110]$

satisfied

↓

If yes, increase count for the key candidate

Will be done for all chosen Plaintext/Ciphertext couples which satisfies

$\Delta P = [0000\ \ 1011\ \ 0000\ \ 0000])$

Will be done for 2^8 possible key candidate

Extracting Key Bits

Prob = count/5000

$$\text{Expected probablity} = \frac{27}{1024} = 0.0264$$

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob	*partial subkey* $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob
1 C	0.0000	2 A	0.0032
1 D	0.0000	2 B	0.0022
1 E	0.0000	2 C	0.0000
1 F	0.0000	2 D	0.0000
2 0	0.0000	2 E	0.0000
2 1	0.0136	2 F	0.0000
2 2	0.0068	3 0	0.0004
2 3	0.0068	3 1	0.0000
2 4	**0.0244**	3 2	0.0004
2 5	0.0000	3 3	0.0004
2 6	0.0068	3 4	0.0000
2 7	0.0068	3 5	0.0004
2 8	0.0030	3 6	0.0000
2 9	0.0024	3 7	0.0008

Table 8. Experimental Results for Differential Attack

Complexity of Attack

$$Fewer\ active\ S - boxes\ \Rightarrow Larger\ Characteristic\ probability$$

$$Number\ of\ required\ plaintext\ \text{pairs} \approx \frac{c}{Differential\ characteristic\ probability}$$

$$i.e\ \ \frac{1024}{27} * c = 37{,}9 * c\ plaintext\ pairs\ enough\ to\ give\ count\ for\ corrent\ key$$

References

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