Differential Cryptanalysis of SPN

Math 4175

§4.4. Differential Cryptanalysis (Biham and Shamir, 1991)

In this section, we will learn another mode of attack, called Differential Cryptanalysis, on SPN.

As we did in Linear Cryptanalysis, we will illustrate this method by using our particular example of SPN cipher.

Differential cryptanalysis involves comparing the X-or operation of two inputs to the X-or operation of the corresponding two outputs. In general, we will consider two (binary strings) inputs x and x^* having a fixed X-or value, denoted by x', that is, $x' = x \oplus x^*$.

Similar to Linear Cryptanalysis, let us suppose that Oscar knows the type of (SPN) cipher and he also has knowledge of a sizable amount of plaintext elements x and x^* with fixed X-or value $x' = x \oplus x^*$ and the corresponding ciphertext elements y and y^* which are encrypted from x and x^* respectively, by using the same unknown key K.

§4.4. Differential Cryptanalysis

Notations: Let $\pi_S : \{0,1\}^m \to \{0,1\}^m$ be an S-box (in our example, $m = 4$).

Let (x, x^*) be a pair of input strings such that $x \oplus x^* = x'$, which is called the input difference. As indicated, we will fix the input difference.

Let $(y, y^*) = (\pi_S(x), \pi_S(x^*))$. Then the output difference is given by $y' = y \oplus y^*$.

In an ideally randomizing cipher, the probability that a particular output difference y' occurs given a particular input difference x' is $\frac{1}{2^m}$, where m is the number of bits of x.

Differential cryptanalysis seeks to exploit a scenario where a particular y' occurs given a particular input difference x' with a very high probability (i.e., much greater than $\frac{1}{2^m}$). The pair (x', y') is referred to as a differential.

§4.4. Differential Cryptanalysis

- For any fixed $x' \in \{0,1\}^m$, define the set $\Delta(x')$ as follows:

$$\Delta(x') = \{(x, x^*) | x \oplus x^* = x'\}$$

- $x \oplus x^* = x' \implies x \oplus x \oplus x^* = x \oplus x' \implies x^* = x \oplus x'$
- Therefore, $\Delta(x') = \{(x, x \oplus x') : x \in \{0,1\}^m\}$.
- $\Delta(x')$ has exactly 2^m elements.
- For each pair in $\Delta(x')$, we can compute the output difference of the S-box (as indicated in the next slide) and tabulate the resulting distribution of output differences. A non-uniform output distribution will be the basis for a successful differential attack.

§4.4. An Example of Output Difference Distribution

When input difference is $x' = 1011$:

x	x^*	y	y^*	y'
0000	1011	1110	1100	0010
0001	1010	0100	0110	0010
0010	1001	1101	1010	0111
0011	1000	0001	0011	0010
0100	1111	0010	0111	0101
0101	1110	1111	0000	1111
0110	1101	1011	1001	0010
0111	1100	1000	0101	1101
1000	0011	0011	0001	0010
1001	0010	1010	1101	0111
1010	0001	0110	0100	0010
1011	0000	1100	1110	0010
1100	0111	0101	1000	1101
1101	0110	1001	1011	0010
1110	0101	0000	1111	1111
1111	0100	0111	0010	0101

sboxSPN.png

§3.4. An Example of Output Difference Distribution

Looking at the last column of the above table, we obtain the following distribution for output difference:

y'	0000	0001	0010	0011	0100	0101	0110	0111
freq.	0	0	8	0	0	2	0	2

y'	1000	1001	1010	1011	1100	1101	1110	1111
freq.	0	0	0	0	0	2	0	2

Only five of the 16 possible output differences actually occur.This particular example has a very non-uniform distribution.

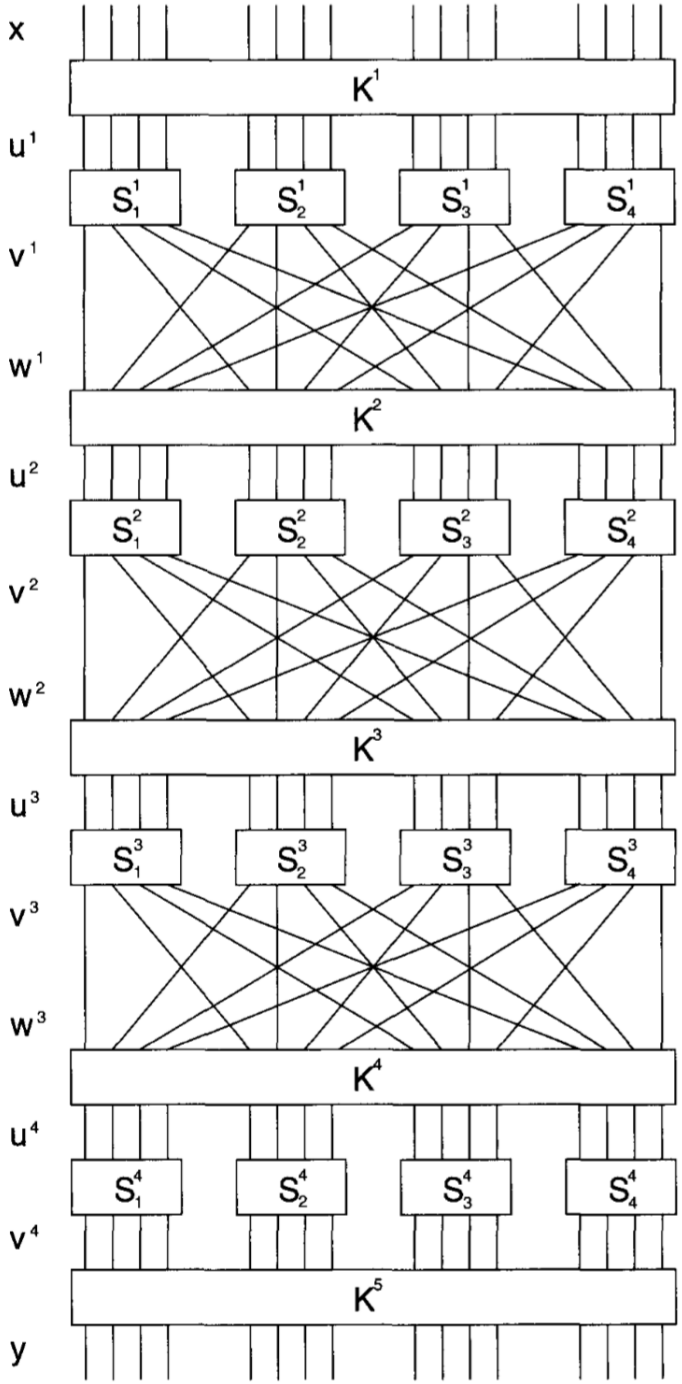
For any particular differences x' and y' define:

$$N_D(x', y') = |\{(x, x^*) \in \Delta(x') : y \oplus y^* = y'\}|$$

$N_D(x', y')$ counts the number of pairs with input difference equal to x' and output difference equal to y' (for a given S-box).

§4.4. Difference Distribution Table: $N_D(a', b')$

a' \ b'	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


x
K1
u1
S11 S21 S31 S41
v1
w1
K2
u2
S12 S22 S32 S42
v2
w2
K3
u3
S13 S23 S33 S43
v3
w3
K4
u4
S14 S24 S34 S44
v4
K5
y

§4.4. Differential Cryptanalysis

If $\alpha \oplus \alpha^* = \alpha'$ then $(\alpha \oplus \beta) \oplus (\alpha^* \oplus \beta) = \alpha'$. So, if α' is fixed, then

$$(\alpha \oplus \beta)^* = \alpha^* \oplus \beta.$$

Recall that the input of the ith S-box in round r of the SPN in our example is denoted by $u^r_{\langle i \rangle}$, and

$$u^r_{\langle i \rangle} = w^{r-1}_{\langle i \rangle} \oplus K^r_{\langle i \rangle}$$

An input difference is computed as

$$u^r_{\langle i \rangle} \oplus \left(u^r_{\langle i \rangle}\right)^* = (w^{r-1}_{\langle i \rangle} \oplus K^r_{\langle i \rangle}) \oplus (w^{r-1}_{\langle i \rangle} \oplus K^r_{\langle i \rangle})^* = w^{r-1}_{\langle i \rangle} \oplus \left(w^{r-1}_{\langle i \rangle}\right)^*$$

Therefore, the input difference does not depend on the round key bits at round r; it is equal to the output difference of round $r-1$.

§4.4. Propagation Ratio

- Recall that a pair (a', b') is called a differential.
- The propagation ratio of a differential is defined as follows:

$$R_p(a', b') = \frac{N_D(a', b')}{2^m}$$

  which is the conditional probability that the output difference is b' given that the input difference is a'.

- For our SPN example:

$$R_p(a', b') = \frac{N_D(a', b')}{2^4}$$

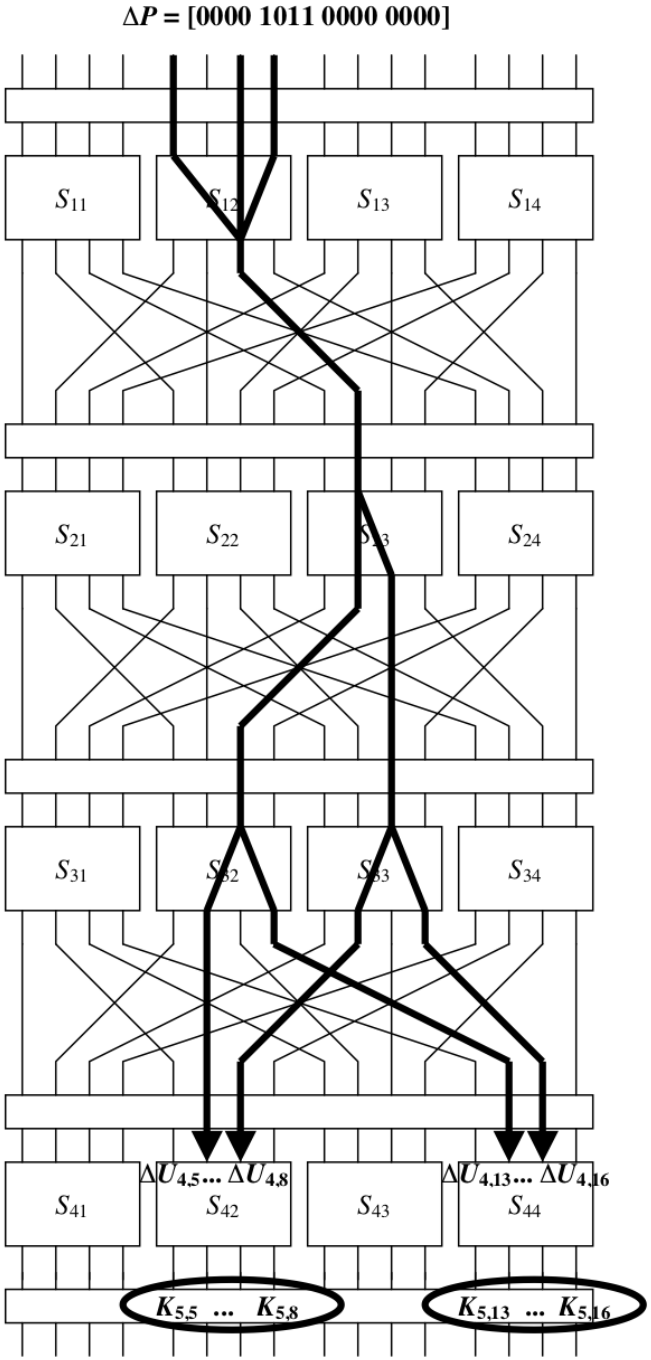
We outline a differential attack which uses the following propagation ratios of differentials:

- In S_2^1, $R_p(1011, 0010) = 1/2$.
- In S_3^2, $R_p(0100, 0110) = 3/8$.
- In S_2^3, $R_p(0010, 0101) = 3/8$.
- In S_3^3, $R_p(0010, 0101) = 3/8$.

All other S-boxes will have zero input **x**-or and consequently zero output **x**-or.
The input **x**-or to the cipher is equivalent to the input **x**-or to the first round and is given by

$$x' = [0000 \quad 1011 \quad 0000 \quad 0000]$$

difftrial.png


ΔP = [0000 1011 0000 0000]
S11
S12
S13
S14
S21
S22
S23
S24
S31
S32
S33
S34
S41
S42
S43
S44
ΔU4,5... ΔU4,8
ΔU4,13... ΔU4,16
K5,5 ... K5,8
K5,13 ... K5,16

The input **x**-or to the cipher is equivalent to the input **x**-or to the first round and is given by

$$x' = [0000 \quad 1011 \quad 0000 \quad 0000]$$

Following the diagram we have

- $(u^1)' = [0000 \quad 1011 \quad 0000 \quad 0000]$
- $(v^1)' = [0000 \quad 0010 \quad 0000 \quad 0000]$
- $(u^2)' = [0000 \quad 0000 \quad 0100 \quad 0000]$
- $(v^2)' = [0000 \quad 0000 \quad 0110 \quad 0000]$
- $(u^3)' = [0000 \quad 0010 \quad 0010 \quad 0000]$
- $(v^3)' = [0000 \quad 0101 \quad 0101 \quad 0000]$

difftrial.png

§4.4. Differential Attack

As indicated in the previous diagram, the selected differentials can be combined to form a differential trail. By assuming the independence, we therefore obtain a propagation ratio for the differential trail of the first three rounds of our SPN.

$$R_p(0000\ \ 1011\ \ 0000\ \ 0000, 0000\ \ 0101\ \ 0101\ \ 0000) = \frac{1}{2}\left(\frac{3}{8}\right)^3 = \frac{27}{1024}$$

In other words, $x' = [0000\ \ 1011\ \ 0000\ \ 0000]$ implies

$$(v^3)' = [0000\ \ 0101\ \ 0101\ \ 0000]$$

with probability $27/1024$.

However,

$$(v^3)' = [0000\ \ 0101\ \ 0101\ \ 0000] \Leftrightarrow (u^4)' = [0000\ \ 0110\ \ 0000\ \ 0110]$$

§4.4. Differential Attack

So, $x' = [0000 \;\; 1011 \;\; 0000 \;\; 0000]$ implies

$$(u^4)' = [0000 \;\; 0110 \;\; 0000 \;\; 0110]$$

with probability 27/1024.

Note that $(u^4)'$ is the **x**-or of two inputs to the last round of S-boxes.

Differential cryptanalysis is a chosen-plaintext attack. We assume that the attacker has a large number of 4-tuples (x, x^*, y, y^*), where the **x**-or value $x' = x \oplus x^*$ is fixed, in our example $x' = 0000 \;\; 1011 \;\; 0000 \;\; 0000$.

The plaintext elements (i.e., x and x^*) are encrypted using the same unknown key, K, yielding the ciphertexts y and y^*.

§4.4. Differential Attack

Filtering Operation: Each 4-tuple (x, x^*, y, y^*), for which the differential holds are often called the right pairs. It is the right pairs that allow us to determine the relevant key bits. Tuples that are not right pairs do not provide any useful information.

For each tuple (x, x^*, y, y^*), note that if

$$(u^4)' = 0000\ 0110\ 0000\ 0110$$

then $y_{\langle 1 \rangle} = y^*_{\langle 1 \rangle}$ and $y_{\langle 3 \rangle} = y^*_{\langle 3 \rangle}$. If a tuple (x, x^*, y, y^*) does not satisfy these conditions, then we know that it is not a right tuple, and we can discard it.

This filtering process increases the efficiency of the attack.

§4.4. Differential Attack

In order to determine the subkey $(K^5_{\langle 2\rangle}, K^5_{\langle 4\rangle})$, we perform our attack as summarized below:

For each possible candidate subkey (L_2, L_4), initialize the counter to zero.

For each tuple $(x, x^*, y, y^*) \in \mathcal{J}$, we first perform the filtering operation. If (x, x^*, y, y^*) is a right tuple, then we compute the following:

For $i = 2$ and 4, let $v^4_{\langle i\rangle} = L_i \oplus y_{\langle i\rangle}$ and then $u^4_{\langle i\rangle} = \pi_S^{-1}\left(v^4_{\langle i\rangle}\right)$.

Similarly, let $\left(v^4_{\langle i\rangle}\right)^* = L_i \oplus (y_{\langle i\rangle})^*$ and then $\left(u^4_{\langle i\rangle}\right)^* = \pi_S^{-1}\left((v^4_{\langle i\rangle})^*\right)$.

Then compute $\left(u^4_{\langle i\rangle}\right)' = u^4_{\langle i\rangle} \oplus \left(u^4_{\langle i\rangle}\right)^*$.

If $\left(u^4_{\langle 2\rangle}\right)' = 0110$ and $\left(u^4_{\langle 4\rangle}\right)' = 0110$, then increment the counter.

After repeating this counting process for all 4-tuples $(x, x^*, y, y^*) \in \mathcal{J}$ and for all the candidate keys, the key with maximum count will be the relevant subkey.

§4.4. Differential Attack

For example, let us check the counter for the subkey $K = 0110\,0011$.

Suppose that $y_{\langle 2\rangle} = 0001$, $y_{\langle 4\rangle} = 0101$, $y^*_{\langle 2\rangle} = 1100$, and $y^*_{\langle 4\rangle} = 0110$.

Then $v^4_{\langle 2\rangle} = 0001 \oplus 0110 = 0111 = 7$, $v^4_{\langle 4\rangle} = 0101 \oplus 0011 = 0110 = 6$, $(v^4_{\langle 2\rangle})^* = 1100 \oplus 0110 = 1010 = A$, $(v^4_{\langle 4\rangle})^* = 0110 \oplus 0011 = 0101 = 5$.

So $u^4_{\langle 2\rangle} = \pi_S^{-1}(7) = F$, $u^4_{\langle 4\rangle} = \pi_S^{-1}(6) = A$, $(u^4_{\langle 2\rangle})^* = \pi_S^{-1}(A) = 9$, and $(u^4_{\langle 4\rangle})^* = \pi_S^{-1}(5) = C$.

Hence $(u^4_{\langle 2\rangle})' = F \oplus 9 = 1111 \oplus 1001 = 0110$ and $(u^4_{\langle 4\rangle})' = A \oplus C = 1010 \oplus 1100 = 0110$.

So we increase the counter in this case.

§4.4. Differential Attack

Remarks:

1. A differential attack based on a differential trail having propagation ratio equal to ϵ will often be successful if the number of tuples, which we denote by $|\mathcal{J}|$, is approximately $c\epsilon^{-1}$, for a small constant c.
2. In our example, $\epsilon^{-1} \approx 38$.
3. For our example, experiments indicate that an attack was often successful for $1.3 \leq c \leq 2.6$ and hence $50 \leq |\mathcal{J}| \leq 100$.

§4.4. Differential Attack

Differential Attack (τ, T, π_S^{-1})**:**

for $(L_1, L_2) \leftarrow (0,0)$ to (F, F) **do** $\text{Count}[L_1, L_2] \leftarrow 0$
for each $(x, y, x^*, y^*) \in \tau$ **do**
if $y_{<1>} = (y_{<1>})^*$ **and** $y_{<3>} = (y_{<3>})^*$

then
- **for** $(L_1, L_2) \leftarrow (0,0)$ **to** (F, F)
- **do**
  - $v^4_{<2>} \leftarrow L_1 \oplus y_{<2>}$, $v^4_{<4>} \leftarrow L_2 \oplus y_{<4>}$
  - $u^4_{<2>} \leftarrow \pi_S^{-1}(v^4_{<2>})$, $u^4_{<4>} \leftarrow \pi_S^{-1}(v^4_{<4>})$
  - $(v^4_{<2>})^* \leftarrow L_1 \oplus (y_{<2>})^*$, $(v^4_{<4>})^* \leftarrow L_2 \oplus (y_{<4>})^*$
  - $(u^4_{<2>})^* \leftarrow \pi_S^{-1}((v^4_{<2>})^*)$, $(u^4_{<4>})^* \leftarrow \pi_S^{-1}((v^4_{<4>})^*)$
  - $(u^4_{<2>})' \leftarrow u^4_{<2>} \oplus (u^4_{<2>})^*$, $(u^4_{<4>})' \leftarrow u^4_{42>} \oplus (u^4_{<4>})^*$
  - **if** $(u^4_{<2>})' = 0110$ **and** $(u^4_{<4>})' = 0110$
  - **then** $\text{Count}[L_1, L_2] \leftarrow \text{Count}[L_1, L_2] + 1$

§4.4. Differential Attack

Linear Attack (τ, T, π_S^{-1}) **continues:**

$\max \leftarrow -1$

for $(L_1, L_2) \leftarrow (0,0)$ **to** (F, F)

do
- $\text{Count}[L_1, L_2] \leftarrow |\text{Count}[L_1, L_2] - T/2|$
- **if** $\text{Count}[L_1, L_2] > \max$
- **then**
  - $\max \leftarrow \text{Count}[L_1, L_2]$
  - $\text{maxkey} \leftarrow (L_1, L_2)$

output (maxkey)