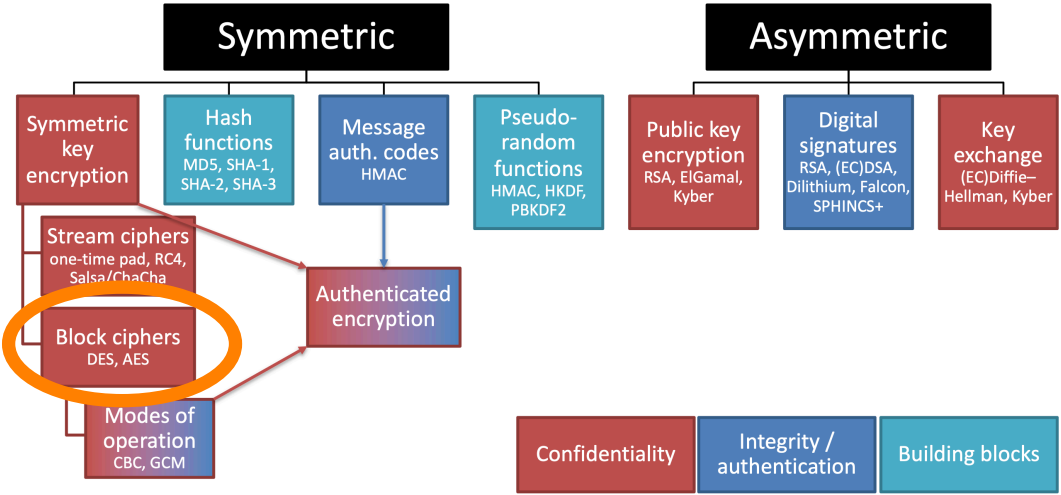
Topic 1.3
Symmetric encryption – Cryptanalysis of block ciphers

Douglas Stebila

CO 487/687: Applied Cryptography
Fall 2024

Map of cryptographic primitives



Linear cryptanalysis

Differential cryptanalysis

- Differential Cryptanalysis of DES

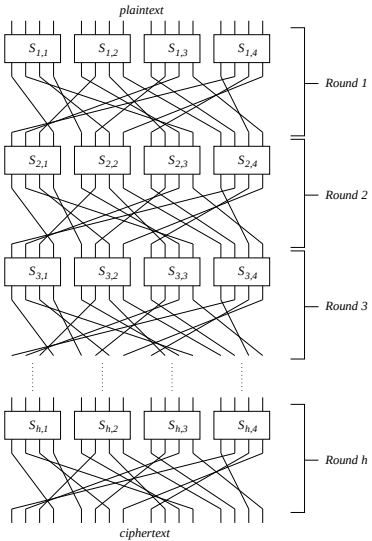
Outline

Substitution-Permutation Networks

A substitution-permutation network (SPN) is a type of iterated block cipher where a round consists of:

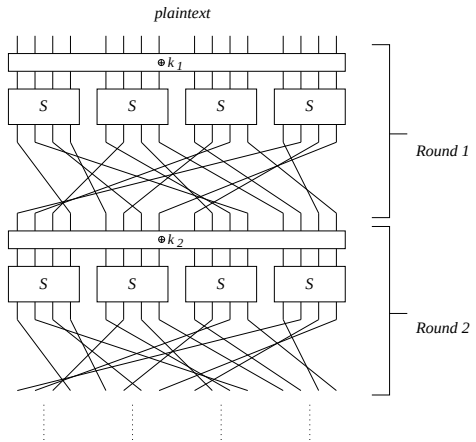
- Incorporation of the round key, followed by
- A substitution operation, followed by
- A permutation operation.

The component function in DES is of this form.



Substitution-Permutation Networks

- The key k influences the result of the substitution step.
- One technique is to XOR the S-box inputs with key bits before the S-box is applied.
- From k, one derives round keys $k_1, k_2, \ldots, k_h, k_{h+1}$ using a key scheduling algorithm. (h denotes the number of rounds)



Examples

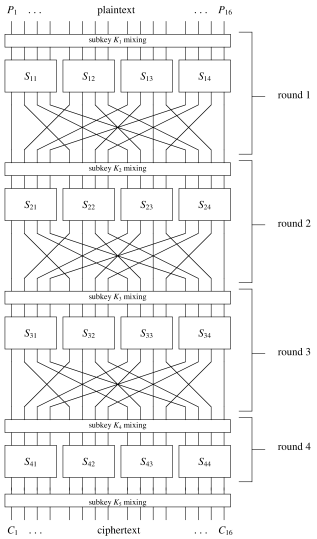
Examples of Substitution-Permutation Network designs:

- Rijndael (AES)
  - Widely used in present-day applications
- Heys cipher
  - Howard M. Heys, “A Tutorial in Linear and Differential Cryptanalysis, ” Cryptologia **26** (3), pp. 189–221, 2002.
  - Simplified cipher, designed for learning purposes

The Heys cipher

Howard M. Heys, “A Tutorial in Linear and Differential Cryptanalysis”

- 4-round SPN
- 16-bit block size
- All S-boxes are identical
- All permutations are identical
- No key schedule algorithm
  (each round’s subkey is independently chosen)
- 80-bit key



The Heys cipher

S-box:

In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Out	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7

Permutation:

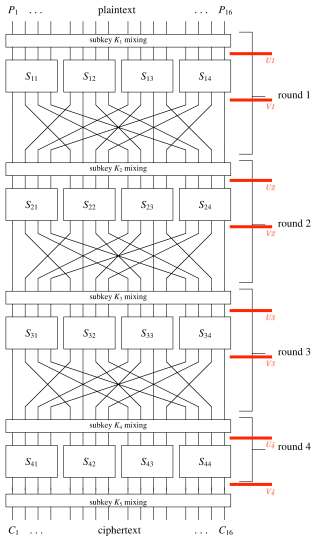
In	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Out	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

- S-box is identical to the first line of the DES S_1 S-box
- Permutation is the “butterfly” or “transpose” permutation
- The K_5 subkey prevents an adversary from reversing the final round of substitution and permutation. In general this technique is called key whitening.

Notation

- Let P denote the plaintext.
- Let C denote the ciphertext.
- Let K_i denote the i-th subkey.
- Let U_i represent the 16-bit block of bits at the input of the i-th round of S-boxes.
- Let V_i represent the 16-bit block of bits at the output of the i-th round of S-boxes.

Note: P, C, K_i, U_i, V_i are all vectors.



Example encryption

- Take the plaintext $P =$ 0110 1001 1101 1011.
- Suppose the key consists of all 1's ($K_i =$ 1111 1111 1111 1111 for $i = 1, 2, 3, 4, 5$)

P	0110 1001 1101 1011
U_1	1001 0110 0010 0100
V_1	1010 1011 1101 0010
U_2	0001 1101 0010 1001
V_2	0100 1001 1101 1010
U_3	1000 0101 1110 1001
V_3	0011 1111 0000 1010
U_4	1010 1011 0010 0011
V_4	0110 1100 1101 0001
C	1001 0011 0010 1110

Linear cryptanalysis

Mitsuru Matsui, “Linear cryptanalysis method for DES cipher,” Advances in Cryptology—EUROCRYPT 1993, pp. 386–397

- The basic idea is to look for linear (boolean) relations among the plaintext/ciphertext/key bits which hold with probability much different from 50%, then use a known plaintext attack to figure out the mostly key.

Linear cryptanalysis

Mitsuru Matsui, “Linear cryptanalysis method for DES cipher,” Advances in Cryptology—EUROCRYPT 1993, pp. 386–397

- The basic idea is to look for linear (boolean) relations among the plaintext/ciphertext/key bits which hold with probability much different from 50%, then use a known plaintext attack to figure out the mostly key.
- For example:

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

- In the above equation, $U_{4,6}$, $U_{4,8}$, $U_{4,14}$, and $U_{4,16}$ depend only on the ciphertext C and the eight key bits $K_{5,5}, K_{5,6}, K_{5,7}, K_{5,8}, K_{5,13}, K_{5,14}, K_{5,15}, K_{5,16}$.
- Given enough known-plaintext pairs (P, C), guess the appropriate partial subkey bits until a guess is found for which the relation holds with probability much different from 50%, over all the known (P, C)-pairs.

Main idea of linear cryptanalysis

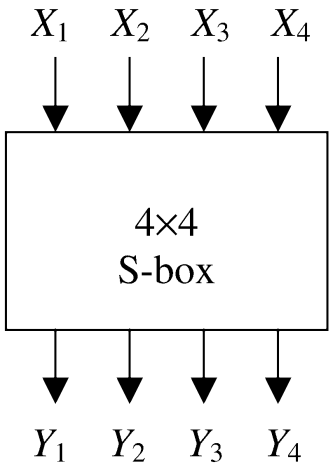
Given many plaintext-ciphertext pairs and a linear relation among the plaintext/ciphertext/key bits which holds with probability much different from 50%

- For the “active” partial subkey bits, go through all possible values:
- For each plaintext-ciphertext pair, record whether the relation holds for these key bits and this plaintext-ciphertext pair.
- The choice of key bits which yields the largest magnitude of bias is probably correct.

Repeat with many different linear relations to recover as much of the key as possible, then use a brute force search on the remaining key bits.

Finding linear relations

- Our goal is to find linear relations which hold with abnormally large or abnormally small probability.
- Start with the S-box!



S-box relations

How often does $X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$?

S-box relations

How often does $X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$?

X	X_1	X_2	X_3	X_4	Y	Y_1	Y_2	Y_3	Y_4
0	0	0	0	0	14	1	1	1	0
1	0	0	0	1	4	0	1	0	0
2	0	0	1	0	13	1	1	0	1
3	0	0	1	1	1	0	0	0	1
4	0	1	0	0	2	0	0	1	0
5	0	1	0	1	15	1	1	1	1
6	0	1	1	0	11	1	0	1	1
7	0	1	1	1	8	1	0	0	0
8	1	0	0	0	3	0	0	1	1
9	1	0	0	1	10	1	0	1	0
10	1	0	1	0	6	0	1	1	0
11	1	0	1	1	12	1	1	0	0
12	1	1	0	0	5	0	1	0	1
13	1	1	0	1	9	1	0	0	1
14	1	1	1	0	0	0	0	0	0
15	1	1	1	1	7	0	1	1	1

S-box relations

How often does $X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$?

X	X_1	X_2	X_3	X_4	Y	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$
0	0	0	0	0	14	1	1	1	0	0	0
1	0	0	0	1	4	0	1	0	0	0	0
2	0	0	1	0	13	1	1	0	1	1	0
3	0	0	1	1	1	0	0	0	1	1	1
4	0	1	0	0	2	0	0	1	0	1	1
5	0	1	0	1	15	1	1	1	1	1	1
6	0	1	1	0	11	1	0	1	1	0	1
7	0	1	1	1	8	1	0	0	0	0	1
8	1	0	0	0	3	0	0	1	1	0	0
9	1	0	0	1	10	1	0	1	0	0	0
10	1	0	1	0	6	0	1	1	0	1	1
11	1	0	1	1	12	1	1	0	0	1	1
12	1	1	0	0	5	0	1	0	1	1	1
13	1	1	0	1	9	1	0	0	1	1	0
14	1	1	1	0	0	0	0	0	0	0	0
15	1	1	1	1	7	0	1	1	1	0	0

S-box relations

How often does $X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$?

X	X_1	X_2	X_3	X_4	Y	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$
0	0	0	0	0	14	1	1	1	0	0	0
1	0	0	0	1	4	0	1	0	0	0	0
2	0	0	1	0	13	1	1	0	1	1	0
3	0	0	1	1	1	0	0	0	1	1	1
4	0	1	0	0	2	0	0	1	0	1	1
5	0	1	0	1	15	1	1	1	1	1	1
6	0	1	1	0	11	1	0	1	1	0	1
7	0	1	1	1	8	1	0	0	0	0	1
8	1	0	0	0	3	0	0	1	1	0	0
9	1	0	0	1	10	1	0	1	0	0	0
10	1	0	1	0	6	0	1	1	0	1	1
11	1	0	1	1	12	1	1	0	0	1	1
12	1	1	0	0	5	0	1	0	1	1	1
13	1	1	0	1	9	1	0	0	1	1	0
14	1	1	1	0	0	0	0	0	0	0	0
15	1	1	1	1	7	0	1	1	1	0	0

S-box relations

- For the S-box from the Heys cipher, the linear relation

$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4$$

  holds with probability $12/16 = 3/4$ and
  fails with probability $4/16 = 1/4$.
- This number is very different from $1/2$!
- The bias of this linear relation is $1/4 = 3/4 - 1/2$.

S-box relations

How often does $X_1 \oplus X_4 = Y_2$?

X	X_1	X_2	X_3	X_4	Y	Y_1	Y_2	Y_3	Y_4	$X_1 \oplus X_4$	Y_2
0	0	0	0	0	14	1	1	1	0	0	1
1	0	0	0	1	4	0	1	0	0	1	1
2	0	0	1	0	13	1	1	0	1	0	1
3	0	0	1	1	1	0	0	0	1	1	0
4	0	1	0	0	2	0	0	1	0	0	0
5	0	1	0	1	15	1	1	1	1	1	1
6	0	1	1	0	11	1	0	1	1	0	0
7	0	1	1	1	8	1	0	0	0	1	0
8	1	0	0	0	3	0	0	1	1	1	0
9	1	0	0	1	10	1	0	1	0	0	0
10	1	0	1	0	6	0	1	1	0	1	1
11	1	0	1	1	12	1	1	0	0	0	1
12	1	1	0	0	5	0	1	0	1	1	1
13	1	1	0	1	9	1	0	0	1	0	0
14	1	1	1	0	0	0	0	0	0	1	0
15	1	1	1	1	7	0	1	1	1	0	1

- $X_1 \oplus X_4 = Y_2$ exactly $1/2$ of the time (no bias).

S-box relations

How often does $X_3 \oplus X_4 = Y_1 \oplus Y_4$?

X	X_1	X_2	X_3	X_4	Y	Y_1	Y_2	Y_3	Y_4	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	0	14	1	1	1	0	0	1
1	0	0	0	1	4	0	1	0	0	1	0
2	0	0	1	0	13	1	1	0	1	1	0
3	0	0	1	1	1	0	0	0	1	0	1
4	0	1	0	0	2	0	0	1	0	0	0
5	0	1	0	1	15	1	1	1	1	1	0
6	0	1	1	0	11	1	0	1	1	1	0
7	0	1	1	1	8	1	0	0	0	0	1
8	1	0	0	0	3	0	0	1	1	0	1
9	1	0	0	1	10	1	0	1	0	1	1
10	1	0	1	0	6	0	1	1	0	1	0
11	1	0	1	1	12	1	1	0	0	0	1
12	1	1	0	0	5	0	1	0	1	0	1
13	1	1	0	1	9	1	0	0	1	1	0
14	1	1	1	0	0	0	0	0	0	1	0
15	1	1	1	1	7	0	1	1	1	0	1

- $X_3 \oplus X_4 = Y_1 \oplus Y_4$ with probability $2/16$.
- The bias is $-6/16 = -3/8$ (negative bias!)

Linear approximation examples

- We have:
  - $X_2 \oplus X_3 \cong Y_1 \oplus Y_3 \oplus Y_4$ with probability $12/16 = 3/4$
  - $X_1 \oplus X_4 \cong Y_2$ with probability $8/16 = 1/2$
  - $X_3 \oplus X_4 \cong Y_1 \oplus Y_4$ with probability $2/16 = 1/8$
- Define the bias of a probability p to be $p - \frac{1}{2}$.
- For the S-box from the Heys cipher,
  - $X_2 \oplus X_3 \oplus Y_1 \oplus Y_3 \oplus Y_4 \cong 0$ with probability $3/4$ (bias $1/4$)
  - $X_1 \oplus X_4 \oplus Y_2 \cong 0$ with probability $1/2$ (bias 0)
  - $X_3 \oplus X_4 \oplus Y_1 \oplus Y_4 \cong 0$ with probability $1/8$ (bias $-3/8$)

Linear approximation table

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

Note use of hexadecimal $0 \ldots F$ to represent 4-bit numbers $0 \ldots 15$

Linear approximation table

How to read this table:

- Linear relation is $a_1 X_1 \oplus a_2 X_2 \oplus a_3 X_3 \oplus a_4 X_4 = b_1 Y_1 \oplus b_2 Y_2 \oplus b_3 Y_3 \oplus b_4 Y_4$.
- $a_i \in \{0,1\}, b_i \in \{0,1\}$ for $i = 1,2,3,4$
- "Input sum" is the value of $a_1 a_2 a_3 a_4$ in binary.
- "Output sum" is the value of $b_1 b_2 b_3 b_4$ in binary.
- The bias of this linear relation is $x/16$ where x is the value of the table cell.

Linear approximation table

How to read this table:

- Linear relation is $a_1 X_1 \oplus a_2 X_2 \oplus a_3 X_3 \oplus a_4 X_4 = b_1 Y_1 \oplus b_2 Y_2 \oplus b_3 Y_3 \oplus b_4 Y_4$.
- $a_i \in \{0,1\}$, $b_i \in \{0,1\}$ for $i = 1,2,3,4$
- "Input sum" is the value of $a_1 a_2 a_3 a_4$ in binary.
- "Output sum" is the value of $b_1 b_2 b_3 b_4$ in binary.
- The bias of this linear relation is $x/16$ where x is the value of the table cell.

For example:

- Consider $X_3 \oplus X_4 \cong Y_1 \oplus Y_4$ (equivalently, $X_3 \oplus X_4 \oplus Y_1 \oplus Y_4 \cong 0$)
- $a_1 a_2 a_3 a_4 = 0011_2 = 3_{10}$
- $b_1 b_2 b_3 b_4 = 1001_2 = 9_{10}$
- Value in table cell is -6.
- Bias is $-6/16 = -3/8$.

Piling-up Lemma

How do probabilities stack as we combine multiple relations?

Piling-up Lemma

How do probabilities stack as we combine multiple relations?

Suppose

- equation 1 holds with probability $p_1 = \frac{1}{2} + \epsilon_1$ (a.k.a., bias ϵ_1) and
- equation 2 holds with probability $p_2 = \frac{1}{2} + \epsilon_2$ (a.k.a., bias ϵ_2),

then, assuming independence, equation 1 and equation 2 *both hold* with probability

$$\frac{1}{2} + 2\epsilon_1\epsilon_2 \quad \text{(bias } 2\epsilon_1\epsilon_2\text{)}$$

Piling-up Lemma

Theorem (Piling-up Lemma (Matsui, 1993))

Let $X_1, X_2, \ldots, X_n$ be independent binary random variables with bias $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ respectively. Then

$$\mathrm{Prob}(X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i.$$

Piling-up Lemma

Theorem (Piling-up Lemma (Matsui, 1993))

Let $X_1, X_2, \ldots, X_n$ be independent binary random variables with bias $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ respectively. Then

$$\mathrm{Prob}(X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i.$$

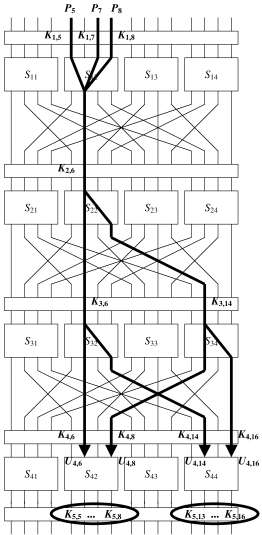
Our inputs are not necessarily independent, but are usually close enough (for practical block ciphers) that the result is close enough.

Constructing linear approximations

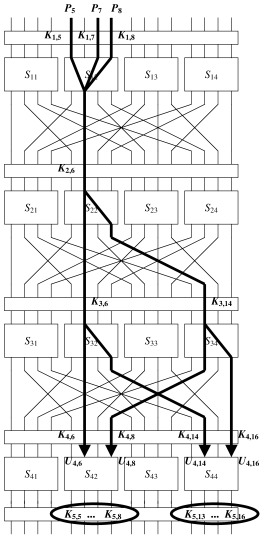
$$
\begin{array}{lccccccc}
S_{12}: & X_1 & & \oplus X_3 & \oplus X_4 & \cong & Y_2 & & \text{(bias } +1/4) \\
S_{22}: & & X_2 & & & \cong & Y_2 & \oplus Y_4 & \text{(bias } -1/4) \\
S_{32}: & & X_2 & & & \cong & Y_2 & \oplus Y_4 & \text{(bias } -1/4) \\
S_{34}: & & X_2 & & & \cong & Y_2 & \oplus Y_4 & \text{(bias } -1/4)
\end{array}
$$

Recall:

- U_i is the 16-bit block of bits at the input of the i-th round of S-boxes.
- V_i is the 16-bit block of bits at the output of the i-th round of S-boxes.
- P is the 16-bit plaintext, C is the 16-bit ciphertext.
- K_i is the 16-bit i-th round subkey.



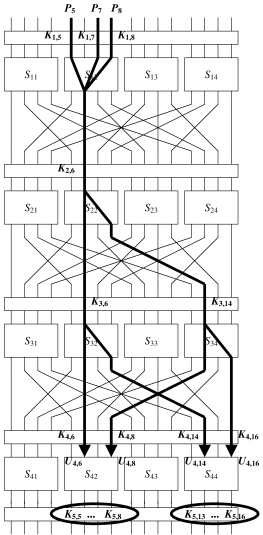
Constructing linear approximations



For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

Constructing linear approximations

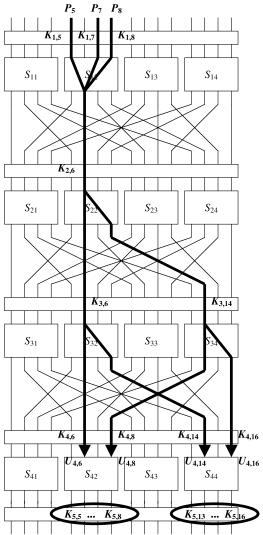


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$U_1 = P \oplus K_1$$

Constructing linear approximations

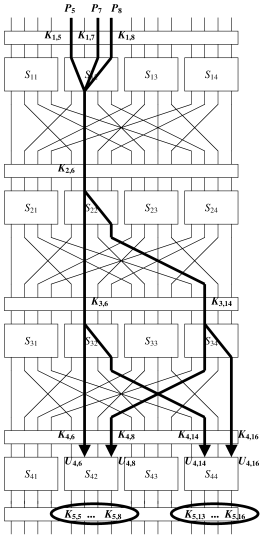


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$\begin{aligned} U_1 &= P \oplus K_1 \\ X_1 &= U_{1,5} = P_5 \oplus K_{1,5} \end{aligned}$$

Constructing linear approximations

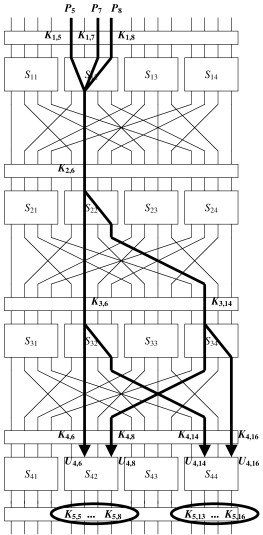


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$\begin{aligned} U_1 &= P \oplus K_1 \\ X_1 &= U_{1,5} = P_5 \oplus K_{1,5} \\ X_3 &= U_{1,7} = P_7 \oplus K_{1,7} \end{aligned}$$

Constructing linear approximations

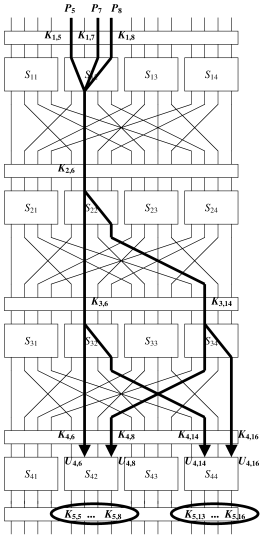


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$\begin{aligned} U_1 &= P \oplus K_1 \\ X_1 &= U_{1,5} = P_5 \oplus K_{1,5} \\ X_3 &= U_{1,7} = P_7 \oplus K_{1,7} \\ X_4 &= U_{1,8} = P_8 \oplus K_{1,8} \end{aligned}$$

Constructing linear approximations

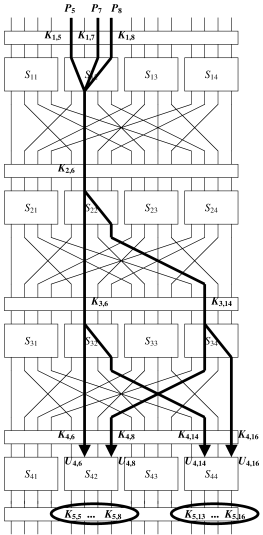


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$\begin{aligned} U_1 &= P \oplus K_1 \\ X_1 &= U_{1,5} = P_5 \oplus K_{1,5} \\ X_3 &= U_{1,7} = P_7 \oplus K_{1,7} \\ X_4 &= U_{1,8} = P_8 \oplus K_{1,8} \\ Y_2 &= V_{1,6} \end{aligned}$$

Constructing linear approximations

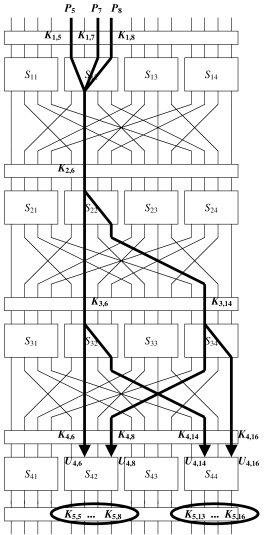


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$\begin{aligned}
U_1 &= P \oplus K_1 \\
X_1 &= U_{1,5} = P_5 \oplus K_{1,5} \\
X_3 &= U_{1,7} = P_7 \oplus K_{1,7} \\
X_4 &= U_{1,8} = P_8 \oplus K_{1,8} \\
Y_2 &= V_{1,6} \\
V_{1,6} &\cong U_{1,5} \oplus U_{1,7} \oplus U_{1,8} \qquad \text{(bias } +1/4)
\end{aligned}$$

Constructing linear approximations

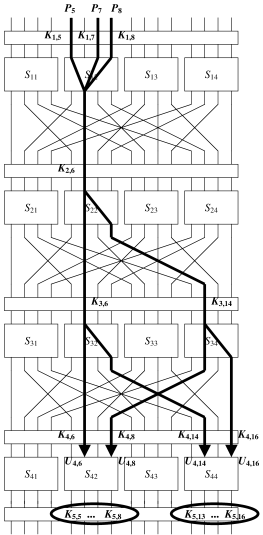


For the approximation:

$$S_{12} : X_1 \oplus X_3 \oplus X_4 \cong Y_2 \qquad \text{(bias } +1/4)$$

$$\begin{aligned}
U_1 &= P \oplus K_1 \\
X_1 &= U_{1,5} = P_5 \oplus K_{1,5} \\
X_3 &= U_{1,7} = P_7 \oplus K_{1,7} \\
X_4 &= U_{1,8} = P_8 \oplus K_{1,8} \\
Y_2 &= V_{1,6} \\
V_{1,6} &\cong U_{1,5} \oplus U_{1,7} \oplus U_{1,8} \qquad \text{(bias } +1/4) \\
&= (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8})
\end{aligned}$$

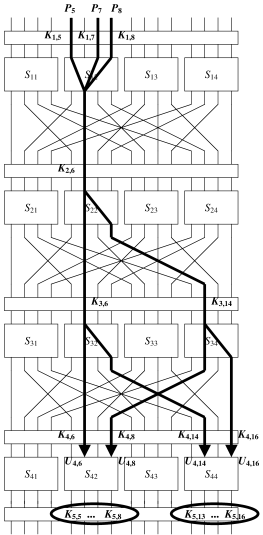
Constructing linear approximations



For the approximation:

$$S_{22} : X_2 \quad \cong \quad Y_2 \oplus Y_4 \qquad (\text{bias } -1/4)$$

Constructing linear approximations

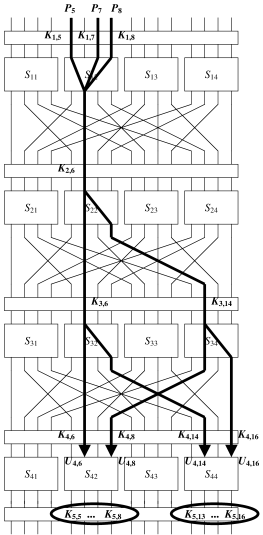


For the approximation:

$$S_{22} : X_2 \quad \cong \quad Y_2 \oplus Y_4 \qquad \text{(bias } -1/4)$$

$$U_{2,6} \quad \cong \quad V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4)$$

Constructing linear approximations



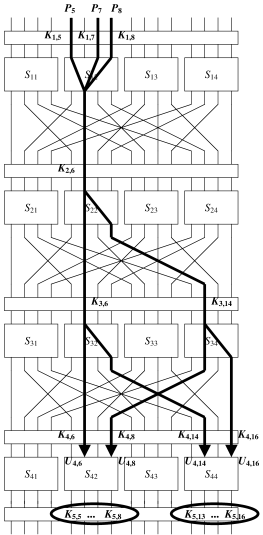
For the approximation:

$$S_{22} : X_2 \cong Y_2 \oplus Y_4 \qquad \text{(bias } -1/4)$$

$$U_{2,6} \cong V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4)$$

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

Constructing linear approximations



For the approximation:

$$S_{22} : X_2 \cong Y_2 \oplus Y_4 \qquad \text{(bias } -1/4)$$

$$U_{2,6} \cong V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4)$$

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

$$V_{1,6} \oplus K_{2,6} \cong V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4)$$

Constructing linear approximations

Combining the two approximations

$$V_{1,6} \oplus K_{2,6} \cong V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4\text{)}$$

$$V_{1,6} \cong P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \qquad \text{(bias } +1/4\text{)}$$

Constructing linear approximations

Combining the two approximations

$$V_{1,6} \oplus K_{2,6} \cong V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4\text{)}$$
$$V_{1,6} \cong P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \qquad \text{(bias } +1/4\text{)}$$

yields:

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \cong 0.$$

Constructing linear approximations

Combining the two approximations

$$V_{1,6} \oplus K_{2,6} \cong V_{2,6} \oplus V_{2,8} \qquad \text{(bias } -1/4\text{)}$$
$$V_{1,6} \cong P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \qquad \text{(bias } +1/4\text{)}$$

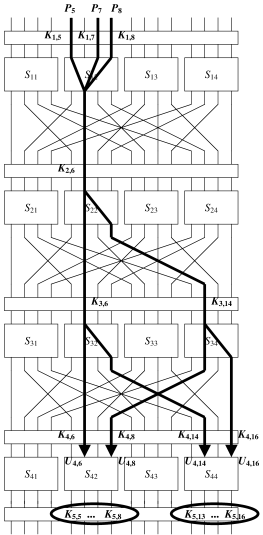
yields:

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \cong 0.$$

By the Piling-up Lemma, this formula holds with bias:

$$2 \cdot \left(-\frac{1}{4}\right) \cdot \left(+\frac{1}{4}\right) = -\frac{1}{8}$$

Constructing linear approximations

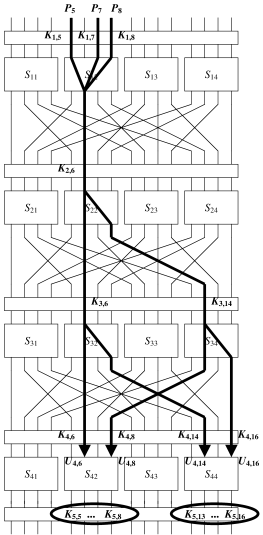


For the approximations:

$$S_{32} : X_2 \quad \cong \quad Y_2 \oplus Y_4 \qquad \text{(bias } -1/4\text{)}$$

$$S_{34} : X_2 \quad \cong \quad Y_2 \oplus Y_4 \qquad \text{(bias } -1/4\text{)}$$

Constructing linear approximations

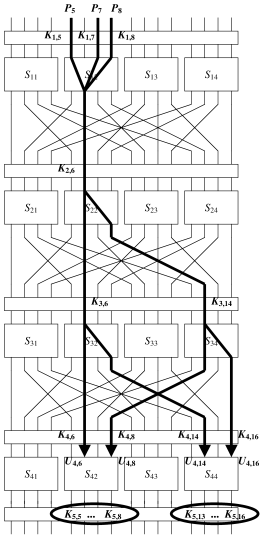


For the approximations:

$$S_{32} : X_2 \quad \cong \quad Y_2 \oplus Y_4 \qquad \text{(bias } -1/4)$$
$$S_{34} : X_2 \quad \cong \quad Y_2 \oplus Y_4 \qquad \text{(bias } -1/4)$$

$$U_{3,6} \quad \cong \quad V_{3,6} \oplus V_{3,8} \qquad \text{(bias } -1/4)$$
$$U_{3,14} \quad \cong \quad V_{3,14} \oplus V_{3,16} \qquad \text{(bias } -1/4)$$

Constructing linear approximations

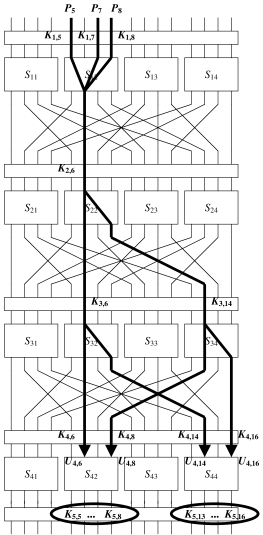


For the approximations:

$$S_{32} : X_2 \cong Y_2 \oplus Y_4 \quad \text{(bias } -1/4\text{)}$$
$$S_{34} : X_2 \cong Y_2 \oplus Y_4 \quad \text{(bias } -1/4\text{)}$$

$$U_{3,6} \cong V_{3,6} \oplus V_{3,8} \quad \text{(bias } -1/4\text{)}$$
$$U_{3,14} \cong V_{3,14} \oplus V_{3,16} \quad \text{(bias } -1/4\text{)}$$
$$U_{3,6} = V_{2,6} \oplus K_{3,6}$$
$$U_{3,14} = V_{2,8} \oplus K_{3,14}$$

Constructing linear approximations



For the approximations:

$$S_{32} : X_2 \cong Y_2 \oplus Y_4 \quad \text{(bias } -1/4\text{)}$$
$$S_{34} : X_2 \cong Y_2 \oplus Y_4 \quad \text{(bias } -1/4\text{)}$$

$$U_{3,6} \cong V_{3,6} \oplus V_{3,8} \quad \text{(bias } -1/4\text{)}$$
$$U_{3,14} \cong V_{3,14} \oplus V_{3,16} \quad \text{(bias } -1/4\text{)}$$
$$U_{3,6} = V_{2,6} \oplus K_{3,6}$$
$$U_{3,14} = V_{2,8} \oplus K_{3,14}$$
$$V_{2,6} \oplus K_{3,6} \cong V_{3,6} \oplus V_{3,8} \quad \text{(bias } -1/4\text{)}$$
$$V_{2,8} \oplus K_{3,14} \cong V_{3,14} \oplus V_{3,16} \quad \text{(bias } -1/4\text{)}$$

Constructing linear approximations

Combining

$$V_{2,6} \oplus K_{3,6} \cong V_{3,6} \oplus V_{3,8} \qquad \text{(bias } -1/4\text{)}$$

$$V_{2,8} \oplus K_{3,14} \cong V_{3,14} \oplus V_{3,16} \qquad \text{(bias } -1/4\text{)}$$

Constructing linear approximations

Combining

$$V_{2,6} \oplus K_{3,6} \cong V_{3,6} \oplus V_{3,8} \qquad \text{(bias } -1/4\text{)}$$
$$V_{2,8} \oplus K_{3,14} \cong V_{3,14} \oplus V_{3,16} \qquad \text{(bias } -1/4\text{)}$$

we obtain

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} \cong 0$$

Constructing linear approximations

Combining

$$V_{2,6} \oplus K_{3,6} \cong V_{3,6} \oplus V_{3,8} \qquad \text{(bias } -1/4\text{)}$$
$$V_{2,8} \oplus K_{3,14} \cong V_{3,14} \oplus V_{3,16} \qquad \text{(bias } -1/4\text{)}$$

we obtain

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} \cong 0$$

with bias

$$2 \cdot \left(-\frac{1}{4}\right) \cdot \left(-\frac{1}{4}\right) = +\frac{1}{8}.$$

Constructing linear approximations

We have

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

with bias $-1/8$ (respectively $+1/8$).

Constructing linear approximations

We have

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

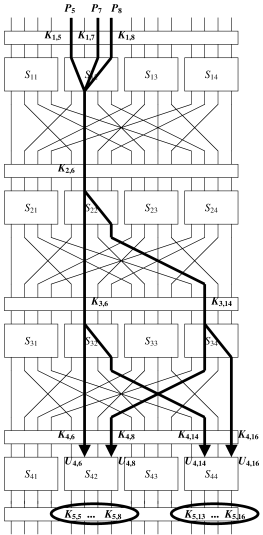
with bias $-1/8$ (respectively $+1/8$). Hence

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

with bias

$$2 \cdot \left(-\frac{1}{8}\right) \cdot \left(+\frac{1}{8}\right) = -\frac{1}{32}.$$

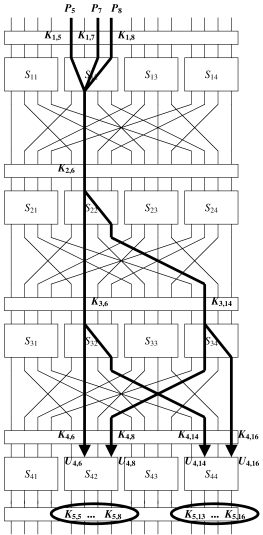
Constructing linear approximations



Combine

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

Constructing linear approximations



Combine

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

with:

$$U_{4,6} = V_{3,6} \oplus K_{4,6}$$
$$U_{4,8} = V_{3,14} \oplus K_{4,8}$$
$$U_{4,14} = V_{3,8} \oplus K_{4,14}$$
$$U_{4,16} = V_{3,16} \oplus K_{4,16}$$

The final approximation

We obtain:

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{4,6} \oplus K_{4,8} \oplus$$
$$K_{4,14} \oplus K_{4,16} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \cong 0.$$

This formula holds with bias $-1/32$.

Once we fix a guess of the key, the key bits are all constant, so we are evaluating the following formula with respect to the known plaintext/ciphertext pairs:

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

which holds with bias $\pm 1/32$.

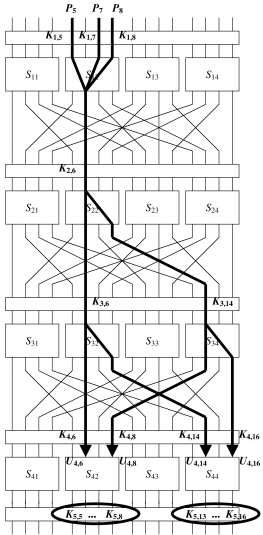
A known-plaintext attack

Given many plaintext-ciphertext pairs:

- Guess the bits $K_{5,5}, K_{5,6}, K_{5,7}, K_{5,8}$ and $K_{5,13}, K_{5,14}, K_{5,15}, K_{5,16}$.
- Using this guess, compute $U_{4,6}, U_{4,8}, U_{4,14}, U_{4,16}$ from C
- Check whether the formula

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

  holds with probability different from 50%, over the plaintext-ciphertext pairs.
- The choice of key bits which yields the largest magnitude of bias is probably correct.

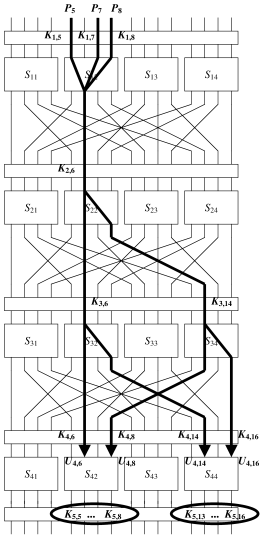


Example

Suppose $P = 0110\ 1001\ 1101\ 1011$ and $C = 1100\ 0110\ 1000\ 1100$.
We guess $K_{5,5} \cdots K_{5,8} = 0111$ and $K_{5,13} \cdots K_{5,16} = 0110$.

$C_5 \cdots C_8$	0110	$C_{13} \cdots C_{16}$	1100
$K_{5,5} \cdots K_{5,8}$	0111	$K_{5,13} \cdots K_{5,16}$	0110
$V_{4,5} \cdots V_{4,8}$	0001	$V_{4,13} \cdots V_{4,16}$	1010
$U_{4,5} \cdots U_{4,8}$	0011	$U_{4,13} \cdots U_{4,16}$	1001

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8$$
$$= 0 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0.$$



Example

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	| bias |	*partial subkey* $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	| 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

This is only a portion of the table. The full table has $2^4 \times 2^4 = 2^8 = 256$ rows for all possible values of the partial subkey in question.

Complexity of linear cryptanalysis

- ϵ: bias from $\frac{1}{2}$ that the linear expression holds for the *complete* cipher
- number of known plaintext-ciphertext pairs required: $\approx 1/\epsilon^2$

Complexity of linear cryptanalysis

- ϵ: bias from $\frac{1}{2}$ that the linear expression holds for the *complete* cipher
- number of known plaintext-ciphertext pairs required: $\approx 1/\epsilon^2$

Implications of this approach:

- The fewer S-boxes involved in a linear approximation, the higher the bias
- Thus, can reduce effectiveness of linear cryptanalysis by designing ciphers that have a high number of “active” S-boxes

Linear cryptanalysis of DES

[Matsui 1993]:

- Recovers key given 2^{43} known plaintext/ciphertext pairs; later improved to $\sim 2^{41}$ pairs.
- Storing these pairs takes 131,000 Gbytes.
- Runtime: 2^{39} to 2^{41} DES evaluations.
- Implemented in 1993: 10 days on 12 machines.
- Implemented in 2001: 3–6 days on idle time of 8–16 computers.

Outline

Differential cryptanalysis

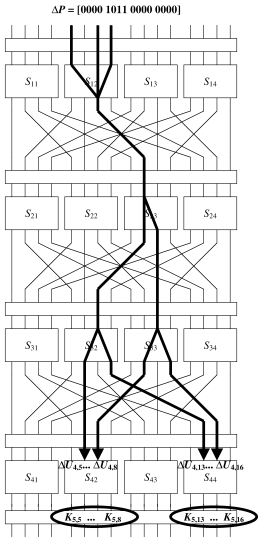
- Eli Biham, Adi Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” CRYPTO 1990.
- Differential cryptanalysis is a *chosen-plaintext attack*. The attacker must choose certain plaintexts strategically and obtain the corresponding ciphertexts.

Idea for differential cryptanalysis

Idea: Look for flaws in the cipher where related plaintexts get encrypted to related ciphertexts. Build up from individual S-boxes.

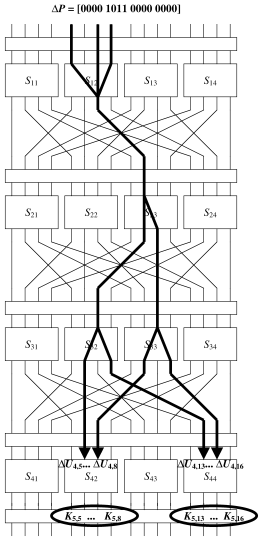
- In a truly random cipher, if two plaintext inputs P and P' are related by some fixed difference $\Delta P = P \oplus P'$, the corresponding ciphertexts C and C' should look completely unrelated.
- But sometimes we see that plaintexts related by some ΔP result in ciphertexts related by some difference $\Delta C = C \oplus C'$.
- A plaintext difference ΔP leading to a ciphertext difference ΔC with better-than-random chance is called a differential characteristic.

Summary of differential cryptanalysis



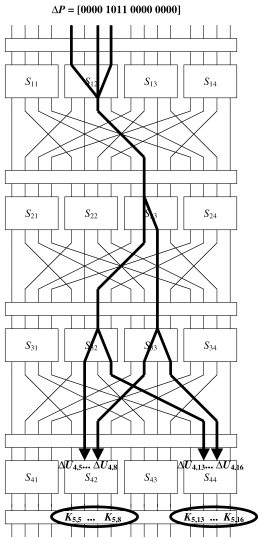
1. Find a differential characteristic from plaintext pairs ΔP to intermediate pairs ΔU_4 that occurs with high probability and involves only a few bits of U_4.

Summary of differential cryptanalysis



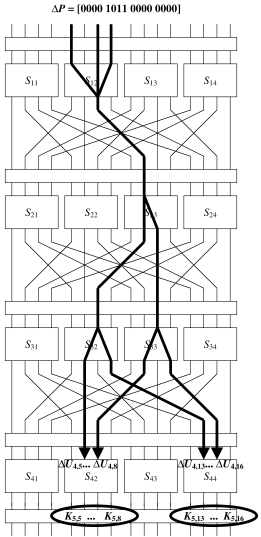
1. Find a differential characteristic from plaintext pairs ΔP to intermediate pairs ΔU_4 that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.

Summary of differential cryptanalysis



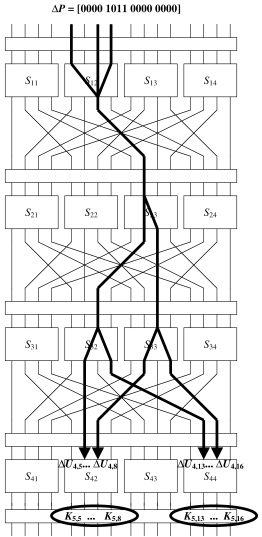
1. Find a differential characteristic from plaintext pairs ΔP to intermediate pairs ΔU_4 that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.
3. Guess the bits of the key that would affect the bits of U_4 appearing in the characteristic.

Summary of differential cryptanalysis



1. Find a differential characteristic from plaintext pairs ΔP to intermediate pairs ΔU_4 that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.
3. Guess the bits of the key that would affect the bits of U_4 appearing in the characteristic.
4. Under this guess, observe how many chosen plaintext pairs satisfy the characteristic.

Summary of differential cryptanalysis



1. Find a differential characteristic from plaintext pairs ΔP to intermediate pairs ΔU_4 that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.
3. Guess the bits of the key that would affect the bits of U_4 appearing in the characteristic.
4. Under this guess, observe how many chosen plaintext pairs satisfy the characteristic.
5. The key guess with the most matching pairs is probably correct.

Overview of differential cryptanalysis

Operation of the attack:

- Let P and P' be two plaintexts.
- Let C and C' be their encryptions.

Overview of differential cryptanalysis

Operation of the attack:

- Let P and P' be two plaintexts.
- Let C and C' be their encryptions.
- Set $\Delta P = P \oplus P'$ and $\Delta C = C \oplus C'$.

Overview of differential cryptanalysis

Operation of the attack:

- Let P and P' be two plaintexts.
- Let C and C' be their encryptions.
- Set $\Delta P = P \oplus P'$ and $\Delta C = C \oplus C'$.
- The idea is to look for values of ΔC which occur with *abnormally high probability* for a given ΔP.

S-box differences

As with linear cryptanalysis, we first perform these steps on the S-box, and gradually scale up to the entire cipher.

- Let X and X' be two plaintexts.
- Let Y and Y' be their encryptions.

S-box differences

As with linear cryptanalysis, we first perform these steps on the S-box, and gradually scale up to the entire cipher.

- Let X and X' be two plaintexts.
- Let Y and Y' be their encryptions.
- Set $\Delta X = X \oplus X'$ and $\Delta Y = Y \oplus Y'$.

S-box differences

As with linear cryptanalysis, we first perform these steps on the S-box, and gradually scale up to the entire cipher.

- Let X and X' be two plaintexts.
- Let Y and Y' be their encryptions.
- Set $\Delta X = X \oplus X'$ and $\Delta Y = Y \oplus Y'$.
- Tabulate, for each ΔX, the possible values for ΔY (much easier for the S-box than for the whole cipher at once!)

S-box differences

As with linear cryptanalysis, we first perform these steps on the S-box, and gradually scale up to the entire cipher.

- Let X and X' be two plaintexts.
- Let Y and Y' be their encryptions.
- Set $\Delta X = X \oplus X'$ and $\Delta Y = Y \oplus Y'$.
- Tabulate, for each ΔX, the possible values for ΔY (much easier for the S-box than for the whole cipher at once!)
- Look for values of ΔY which occur with *abnormally high probability* for a given ΔX.

Difference pairs for the Heys cipher S-box

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	1011	0110
0011	0001	0010	1101	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	1011	0110
1011	1100	0010	1101	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

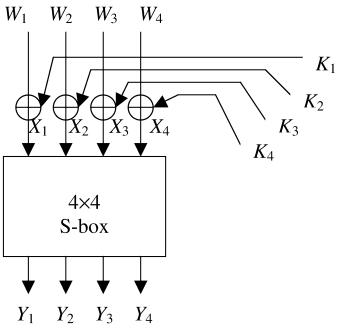
Note table corrects some typos in Heys' original article

Table of difference pairs

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

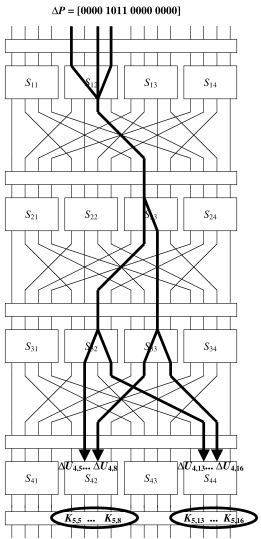
Key considerations

Since the subkey is XOR'ed in before the S-box, it does not affect a plaintext difference pair: the XOR of the subkey in the two plaintexts will cancel out.



$$\Delta X = X \oplus X' = (W \oplus K) \oplus (W' \oplus K) = W \oplus W' = \Delta W.$$

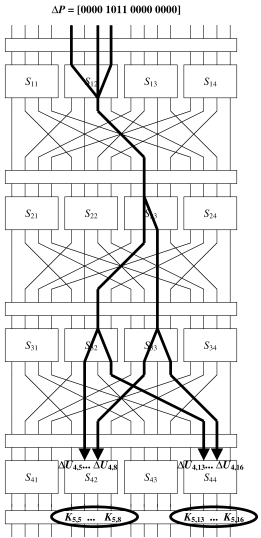
Differential attack



Consider the difference pairs:

$$S_{12} \quad : \quad \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16)$$

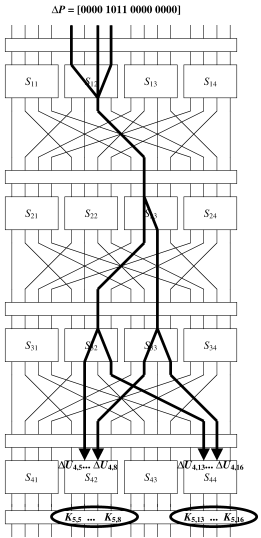
Differential attack



Consider the difference pairs:

$$S_{12} \quad : \quad \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16)$$
$$S_{23} \quad : \quad \Delta X = 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16)$$

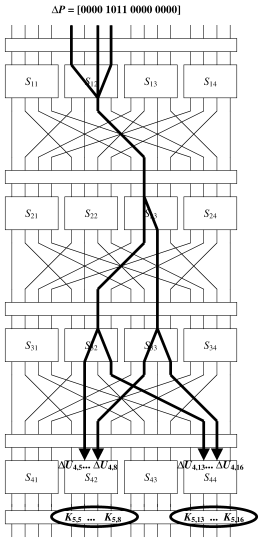
Differential attack



Consider the difference pairs:

$$
\begin{aligned}
S_{12} &: \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16) \\
S_{23} &: \Delta X = 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16) \\
S_{32} &: \Delta X = 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
S_{33} &: \Delta X = 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16)
\end{aligned}
$$

Differential attack

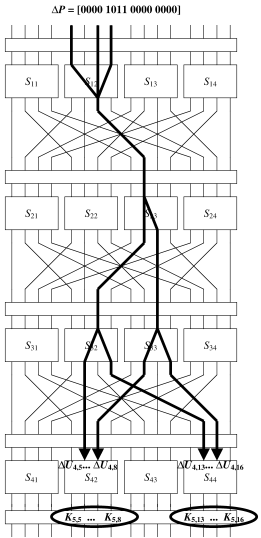


Consider the difference pairs:

$$
\begin{aligned}
S_{12} &: \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16) \\
S_{23} &: \Delta X = 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16) \\
S_{32} &: \Delta X = 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
S_{33} &: \Delta X = 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16)
\end{aligned}
$$

Set $\Delta P = \Delta U_1 = 0000\ 1011\ 0000\ 0000$.

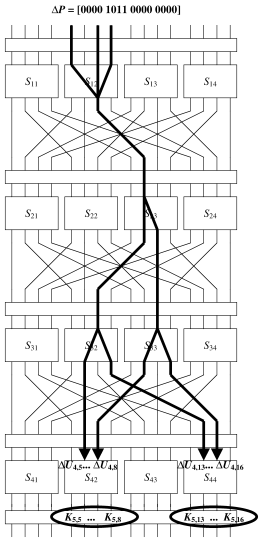
Differential attack



From

$$S_{12} : \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16)$$

Differential attack



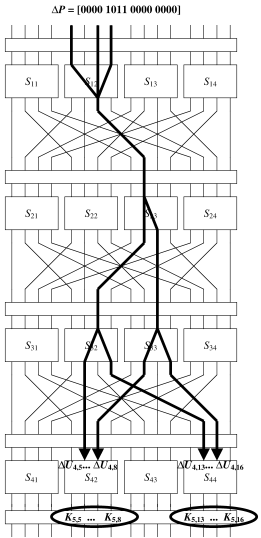
From

$$S_{12} : \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16)$$

we have

$$\Delta P \quad = \quad \Delta U_1 = 0000\ 1011\ 0000\ 0000$$

Differential attack



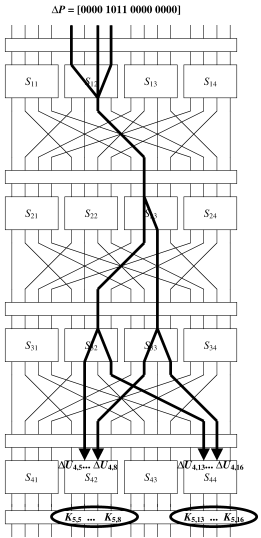
From

$$S_{12} : \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16)$$

we have

$$\begin{aligned} \Delta P &= \Delta U_1 = 0000\ 1011\ 0000\ 0000 \\ \Delta V_1 &= 0000\ 0010\ 0000\ 0000 \text{ (prob. } 8/16) \end{aligned}$$

Differential attack



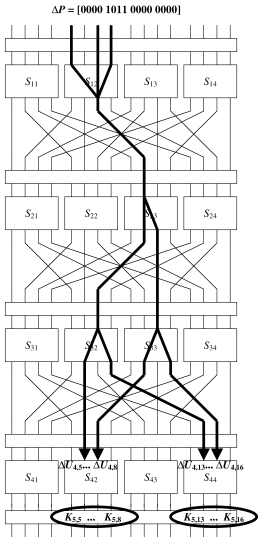
From

$$S_{12} : \Delta X = 1011 \mapsto \Delta Y = 0010 \text{ (prob. } 8/16)$$

we have

$$\begin{aligned} \Delta P &= \Delta U_1 = 0000\ 1011\ 0000\ 0000 \\ \Delta V_1 &= 0000\ 0010\ 0000\ 0000 \text{ (prob. } 8/16) \\ \Delta U_2 &= 0000\ 0000\ 0100\ 0000 \text{ (prob. } 8/16) \end{aligned}$$

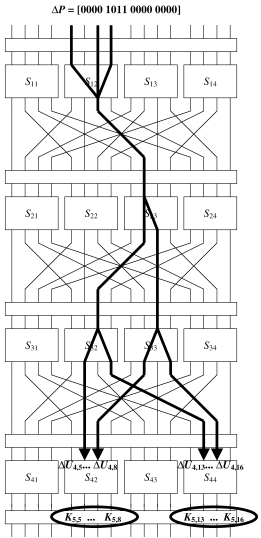
Differential attack



From

$$S_{23} : \Delta X \quad = \quad 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16)$$

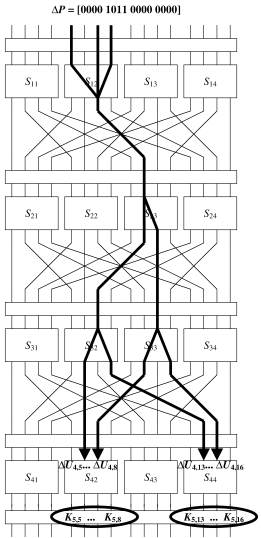
Differential attack



From

$$
\begin{aligned}
S_{23} : \Delta X &= 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16) \\
\Delta U_2 &= 0000\ 0000\ 0100\ 0000 \text{ (prob. } 8/16)
\end{aligned}
$$

Differential attack



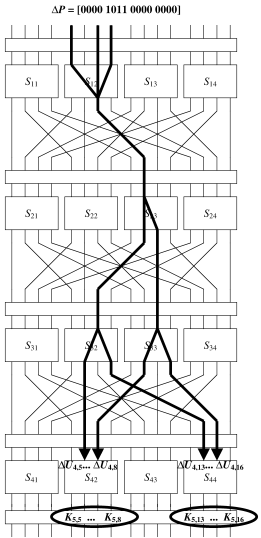
From

$$
\begin{aligned}
S_{23} : \Delta X &= 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16) \\
\Delta U_2 &= 0000\ 0000\ 0100\ 0000 \text{ (prob. } 8/16)
\end{aligned}
$$

we have

$$
\Delta V_2 = 0000\ 0000\ 0110\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16})
$$

Differential attack



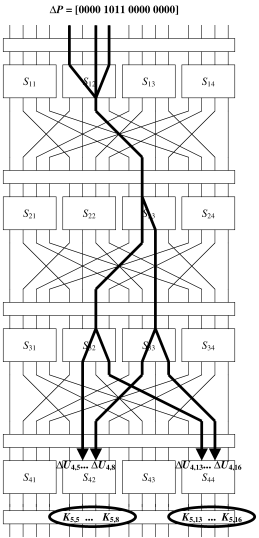
From

$$
\begin{aligned}
S_{23} : \Delta X &= 0100 \mapsto \Delta Y = 0110 \text{ (prob. } 6/16) \\
\Delta U_2 &= 0000\ 0000\ 0100\ 0000 \text{ (prob. } 8/16)
\end{aligned}
$$

we have

$$
\begin{aligned}
\Delta V_2 &= 0000\ 0000\ 0110\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16}) \\
\Delta U_3 &= 0000\ 0010\ 0010\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16})
\end{aligned}
$$

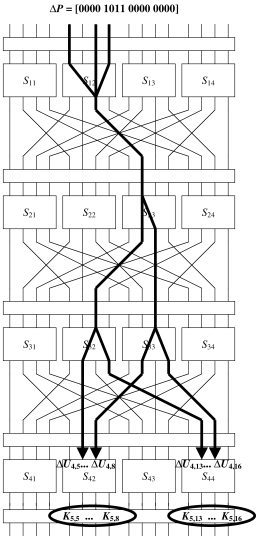
Differential attack



From

$$S_{32} : \Delta X = 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16)$$
$$S_{33} : \Delta X = 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16)$$

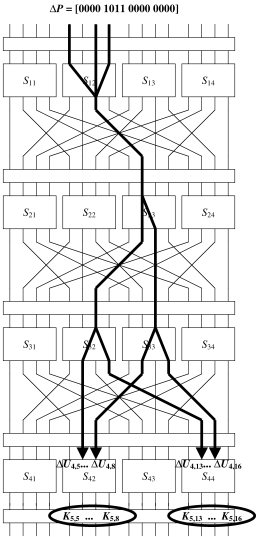
Differential attack



From

$$
\begin{aligned}
S_{32} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
S_{33} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
\Delta U_3 &= 0000\ 0010\ 0010\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16})
\end{aligned}
$$

Differential attack



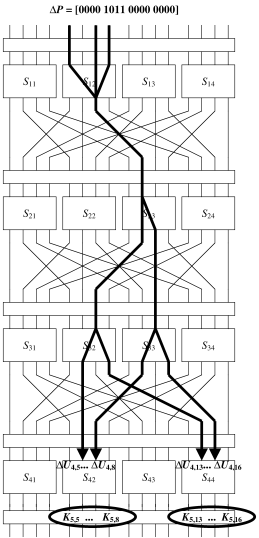
From

$$
\begin{aligned}
S_{32} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
S_{33} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
\Delta U_3 &= 0000\ 0010\ 0010\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16})
\end{aligned}
$$

we have

$$
\Delta V_3 = 0000\ 0101\ 0101\ 0000
$$

Differential attack



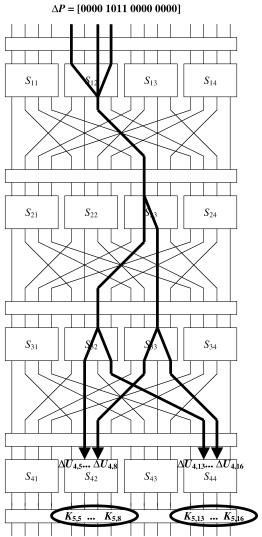
From

$$
\begin{aligned}
S_{32} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
S_{33} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
\Delta U_3 &= 0000\ 0010\ 0010\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16})
\end{aligned}
$$

we have

$$
\begin{aligned}
\Delta V_3 &= 0000\ 0101\ 0101\ 0000 \\
\Delta U_4 &= 0000\ 0110\ 0000\ 0110
\end{aligned}
$$

Differential attack



From

$$
\begin{aligned}
S_{32} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
S_{33} : \Delta X &= 0010 \mapsto \Delta Y = 0101 \text{ (prob. } 6/16) \\
\Delta U_3 &= 0000\ 0010\ 0010\ 0000 \text{ (prob. } \frac{8}{16} \cdot \frac{6}{16})
\end{aligned}
$$

we have

$$
\begin{aligned}
\Delta V_3 &= 0000\ 0101\ 0101\ 0000 \\
\Delta U_4 &= 0000\ 0110\ 0000\ 0110
\end{aligned}
$$

with probability $\frac{8}{16} \cdot \frac{6}{16} \cdot \frac{6}{16} \cdot \frac{6}{16} = \frac{27}{1024}$.

The attack

- A difference $\Delta P = 0000\ 1011\ 0000\ 0000$ in plaintext produces a difference $\Delta U_4 = 0000\ 0110\ 0000\ 0110$ with probability $27/1024$. This probability is *much* higher than uniform.

The attack

- A difference $\Delta P = 0000\ 1011\ 0000\ 0000$ in plaintext produces a difference $\Delta U_4 = 0000\ 0110\ 0000\ 0110$ with probability $27/1024$. This probability is *much* higher than uniform.
- Choose a large number of plaintext pairs with $\Delta P = 0000\ 1011\ 0000\ 0000$ and obtain the corresponding ciphertexts.

The attack

- A difference $\Delta P = 0000\ 1011\ 0000\ 0000$ in plaintext produces a difference $\Delta U_4 = 0000\ 0110\ 0000\ 0110$ with probability $27/1024$. This probability is *much* higher than uniform.
- Choose a large number of plaintext pairs with $\Delta P = 0000\ 1011\ 0000\ 0000$ and obtain the corresponding ciphertexts.
- Guess the values of $K_{5,5}, K_{5,6}, K_{5,7}, K_{5,8}, K_{5,13}, K_{5,14}, K_{5,15}, K_{5,16}$.

The attack

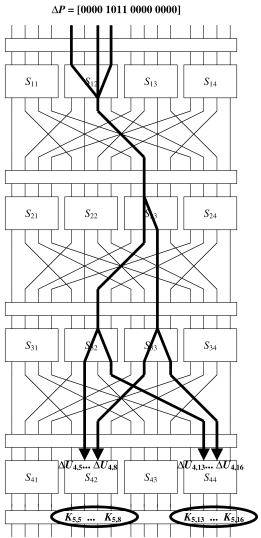
- A difference $\Delta P = 0000\ 1011\ 0000\ 0000$ in plaintext produces a difference $\Delta U_4 = 0000\ 0110\ 0000\ 0110$ with probability $27/1024$. This probability is *much* higher than uniform.
- Choose a large number of plaintext pairs with $\Delta P = 0000\ 1011\ 0000\ 0000$ and obtain the corresponding ciphertexts.
- Guess the values of $K_{5,5}, K_{5,6}, K_{5,7}, K_{5,8}, K_{5,13}, K_{5,14}, K_{5,15}, K_{5,16}$.
- Based on our guess, compute the values of

$$\Delta U_{4,5}, \Delta U_{4,6}, \Delta U_{4,7}, \Delta U_{4,8}, \Delta U_{4,13}, \Delta U_{4,14}, \Delta U_{4,15}, \Delta U_{4,16}$$

The attack

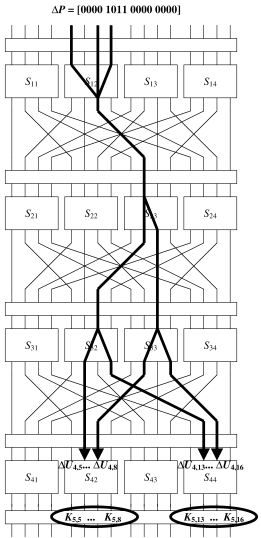
- Under this guess for the partial subkey, count how many plaintext/ciphertext pairs satisfy $\Delta U_4 = 0000\ 0110\ 0000\ 0110$, and see if the count is abnormally large.
- If the count is abnormally large, then our guess for the key bits is probably correct.

Summary of differential cryptanalysis



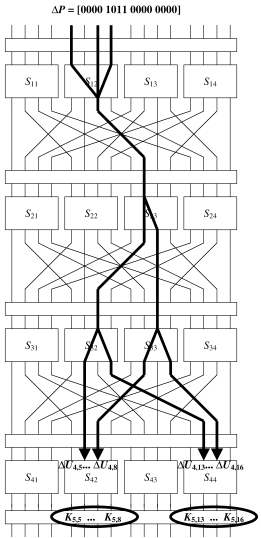
1. Find a differential characteristic $\Delta P \mapsto \Delta U_4$ that occurs with high probability and involves only a few bits of U_4.

Summary of differential cryptanalysis



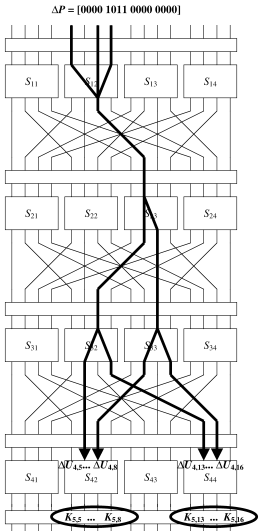
1. Find a differential characteristic $\Delta P \mapsto \Delta U_4$ that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.

Summary of differential cryptanalysis



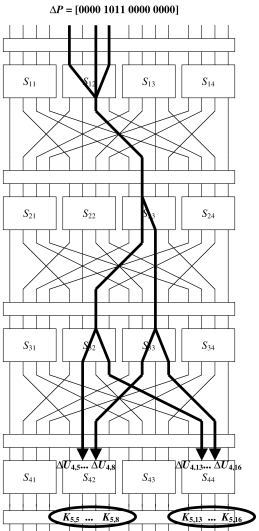
1. Find a differential characteristic $\Delta P \mapsto \Delta U_4$ that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.
3. Guess the bits of the key that would affect the bits of U_4 appearing in the characteristic.

Summary of differential cryptanalysis



1. Find a differential characteristic $\Delta P \mapsto \Delta U_4$ that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.
3. Guess the bits of the key that would affect the bits of U_4 appearing in the characteristic.
4. Under this guess, observe how many chosen plaintext pairs satisfy the characteristic.

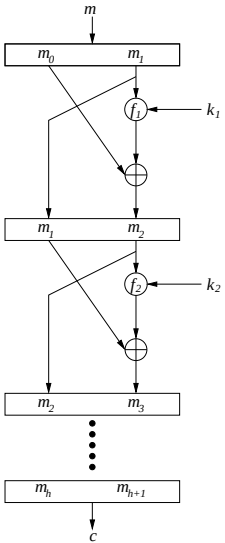
Summary of differential cryptanalysis



1. Find a differential characteristic $\Delta P \mapsto \Delta U_4$ that occurs with high probability and involves only a few bits of U_4.
2. Choose a bunch of plaintext pairs with difference ΔP and obtain the corresponding ciphertexts.
3. Guess the bits of the key that would affect the bits of U_4 appearing in the characteristic.
4. Under this guess, observe how many chosen plaintext pairs satisfy the characteristic.
5. The key guess with the most matching pairs is probably correct.

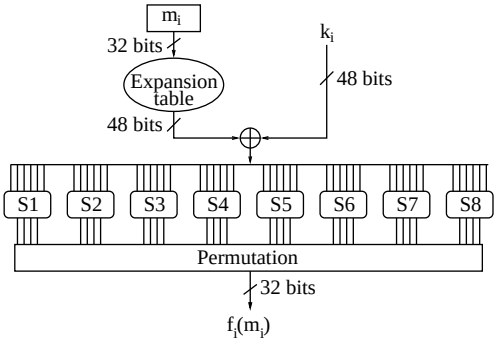
Outline

DES



- Recall the Feistel network design of DES.
- Plaintext is divided into two halves.
- Key is used to generate subkeys $k_1, k_2, \ldots, k_{16}$
- f_i is a *component function* whose output value depends on k_i and m_i.
- We will ignore the initial permutation IP.

DES component function



- Let E denote the expansion table function.
- Let π denote the permutation.

DES overview

- The analogue of U_4 is $U_h = E(m_h) \oplus k_h$.
- The analogue of V_4 is $V_h = \pi^{-1}(m_h \oplus m_{h+1})$.
- Unlike the Heys cipher, no key whitening is used.
- However, the S-box is not one-to-one.

m_0	m_1	$P =$ Plaintext
m_1	m_2	$m_2 = m_0 \oplus f_1(m_1)$
m_2	m_3	$m_3 = m_1 \oplus f_2(m_2)$
m_3	m_4	$m_4 = m_2 \oplus f_3(m_3)$
m_4	m_5	$m_5 = m_3 \oplus f_4(m_4)$
m_5	m_6	$m_6 = m_4 \oplus f_5(m_5)$
m_6	m_7	$m_7 = m_5 \oplus f_6(m_6)$
m_7	m_8	$m_8 = m_6 \oplus f_7(m_7)$
m_8	m_9	$m_9 = m_7 \oplus f_8(m_8)$
m_9	m_{10}	$m_{10} = m_8 \oplus f_9(m_9)$
m_{10}	m_{11}	$m_{11} = m_9 \oplus f_{10}(m_{10})$
m_{11}	m_{12}	$m_{12} = m_{10} \oplus f_{11}(m_{11})$
m_{12}	m_{13}	$m_{13} = m_{11} \oplus f_{12}(m_{12})$
m_{13}	m_{14}	$m_{14} = m_{12} \oplus f_{13}(m_{13})$
m_{14}	m_{15}	$m_{15} = m_{13} \oplus f_{14}(m_{14})$
m_{15}	m_{16}	$m_{16} = m_{14} \oplus f_{15}(m_{15})$
m_{16}	m_{17}	$m_{17} = m_{15} \oplus f_{16}(m_{16})$ $C =$ Ciphertext

Propagation of difference pairs

- Suppose $\Delta P = P \oplus P'$.
- The expansion table is linear: $E(\Delta X) = \Delta(E(X))$.
- The permutation is linear: $\pi(\Delta X) = \Delta(\pi(X))$.
- The round functions are linear: $\Delta m_i = \Delta(m_{i-1} \oplus f_i(m_i)) = \Delta(m_{i-1}) \oplus \Delta(f_i(m_i))$.
- The only non-linear components of DES are the S-boxes.

DES S-boxes

Columns denote middle four bits of input. Rows denote outer two bits of input.

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S-box design principles

The following design principles have been publicly disclosed:

1. Avoid affine or linear functions.
2. A one-bit input difference changes at least two output bits.
3. $S(X)$ and $S(X \oplus 001100)$ differ in at least two bits.
4. $S(X) \neq S(X \oplus 11ab00)$ for all bits a and b.
5. Try to maintain a roughly constant number of 1's and 0's in the output over all inputs where any single input bit is held constant.

The four edge bits are shared between adjacent S-boxes.
The two center bits are never shared!

Differential characteristics of the DES S-boxes

- As for the Heys cipher, we tabulate the differential characteristics of the S-boxes for DES.
- There are eight S-boxes, each with 6 input bits and 4 output bits, for a total of $8 \cdot 2^6 \cdot 2^4 = 2^{13} = 8192$ table entries.

4-round DES

ΔP	20 00 00 00	00 00 00 00	
$\Delta m_1 \| \Delta m_2$	00 00 00 00	20 00 00 00	100% probability
$\Delta m_2 \| \Delta m_3$	20 00 00 00	?0 00 00 00	(ignoring permutation π)

4-round DES

ΔP	20 00 00 00	00 00 00 00	
$\Delta m_1 \| \Delta m_2$	00 00 00 00	20 00 00 00	100% probability
$\Delta m_2 \| \Delta m_3$	20 00 00 00	?0 00 00 00	(ignoring permutation π)

- $C = m_4 || m_5$
- $m_5 = m_3 \oplus f_4(m_4)$
- $m_3 = m_1 \oplus f_2(m_2)$

4-round DES

ΔP	20 00 00 00	00 00 00 00	
$\Delta m_1 \| \Delta m_2$	00 00 00 00	20 00 00 00	100% probability
$\Delta m_2 \| \Delta m_3$	20 00 00 00	?0 00 00 00	(ignoring permutation π)

- $C = m_4 || m_5$
- $m_5 = m_3 \oplus f_4(m_4)$
- $m_3 = m_1 \oplus f_2(m_2)$
- Therefore $\Delta f_4(m_4) = \Delta m_1 \oplus \Delta m_5 \oplus \Delta f_2(m_2)$.

4-round DES

ΔP	20 00 00 00	00 00 00 00	
$\Delta m_1 \| \Delta m_2$	00 00 00 00	20 00 00 00	100% probability
$\Delta m_2 \| \Delta m_3$	20 00 00 00	?0 00 00 00	(ignoring permutation π)

- $C = m_4 || m_5$
- $m_5 = m_3 \oplus f_4(m_4)$
- $m_3 = m_1 \oplus f_2(m_2)$
- Therefore $\Delta f_4(m_4) = \Delta m_1 \oplus \Delta m_5 \oplus \Delta f_2(m_2)$.
  - Δm_1 is known (right half of P – equals zero!)
  - Δm_5 is known (right half of C)
  - $\Delta f_2(m_2) =$?0 00 00 00 is almost zero (equals Δm_3, ignoring the permutation π).

4-round DES

ΔP	20 00 00 00	00 00 00 00	
$\Delta m_1 \| \Delta m_2$	00 00 00 00	20 00 00 00	100% probability
$\Delta m_2 \| \Delta m_3$	20 00 00 00	?0 00 00 00	(ignoring permutation π)

- $C = m_4 || m_5$
- $m_5 = m_3 \oplus f_4(m_4)$
- $m_3 = m_1 \oplus f_2(m_2)$
- Therefore $\Delta f_4(m_4) = \Delta m_1 \oplus \Delta m_5 \oplus \Delta f_2(m_2)$.
  - Δm_1 is known (right half of P – equals zero!)
  - Δm_5 is known (right half of C)
  - $\Delta f_2(m_2) =$?0 00 00 00 is almost zero (equals Δm_3, ignoring the permutation π).
- Find out which choices of the $6 \cdot 7 = 42$ bits of k_4 corresponding to the seven unchanged S-box inputs are consistent with the known values of m_4, m_4', and $\Delta f_4(m_4)$.

4-round DES

ΔP	20 00 00 00	00 00 00 00	
$\Delta m_1 \| \Delta m_2$	00 00 00 00	20 00 00 00	100% probability
$\Delta m_2 \| \Delta m_3$	20 00 00 00	?0 00 00 00	(ignoring permutation π)

- $C = m_4 || m_5$
- $m_5 = m_3 \oplus f_4(m_4)$
- $m_3 = m_1 \oplus f_2(m_2)$
- Therefore $\Delta f_4(m_4) = \Delta m_1 \oplus \Delta m_5 \oplus \Delta f_2(m_2)$.
  - Δm_1 is known (right half of P – equals zero!)
  - Δm_5 is known (right half of C)
  - $\Delta f_2(m_2) =$?0 00 00 00 is almost zero (equals Δm_3, ignoring the permutation π).
- Find out which choices of the $6 \cdot 7 = 42$ bits of k_4 corresponding to the seven unchanged S-box inputs are consistent with the known values of m_4, m_4', and $\Delta f_4(m_4)$.
- Given 42 bits of k_4, you know 42 bits of k. Brute-force the remaining 14 bits.

Cryptanalysis of DES

"DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study."

—Bruce Schneier

Cryptanalysis of DES

"DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study."

—Bruce Schneier

- Brute force attacks (try every key):
  - (1977 estimate) $20 million machine to find keys in one day
  - (1993 estimate) $1 million machine to find keys in 7 hours
  - (1999) EFF DES Cracker: $250,000 machine, 4.5 days per key
  - (2006) COPACOBANA: $10,000 machine, 4.5 days per key
  - (2012) Cloudcracker.com: $200 and 11.5 hours per key

Cryptanalysis of DES

"DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study."

—Bruce Schneier

- Brute force attacks (try every key):
  - (1977 estimate) $20 million machine to find keys in one day
  - (1993 estimate) $1 million machine to find keys in 7 hours
  - (1999) EFF DES Cracker: $250,000 machine, 4.5 days per key
  - (2006) COPACOBANA: $10,000 machine, 4.5 days per key
  - (2012) Cloudcracker.com: $200 and 11.5 hours per key
- Non-brute-force attacks:
  - Differential cryptanalysis (Eli Biham & Adi Shamir, 1991): 2^{49} chosen plaintexts
  - Linear cryptanalysis (Mitsuru Matsui, 1993): 2^{43} known plaintexts