Attack on DES

Jing Li

Major cryptanalytic attacks against DES

- 1976: For a very small class of weak keys, DES can be broken with complexity 1
- 1977: Exhaustive search will become possible within 20 years, breaking DES with complexity 2^{56}
- 1980: A time/memory tradeoff can break DES faster at the expense of more memory
- 1982: For a very small class of semi-weak keys, DES can be broken with complexity 1
- 1985: A meet-in-the-middle attack can break 6-round DES with complexity 2^{52}
- 1987: the "Davies Attack" can break DES with complexity $2^{56.2}$,slightly worse than brute force
- 1990: Differential cryptanalysis can break DES with 2^{47} chosen plaintext (full 16-round)
- 1993: Linear cryptanalysis can break DES with 2^{43} known plaintexts
- 1994: Differential-linear cryptanalysis can break 8-round DES with 768 chosen plaintexts plus 2^{46} a brute-force search
- 1994: the Davies attack can be improved, and can break DES with 2^{52} known plaintexts

Brute-force Attack

The main idea of brute-force attack is systematically checking all possible keys until the correct key is found.

In the worst case, this would involve traversing the entire search space.

It will always find a solution

Attacks faster than Brute-force

Differential Cryptanalysis

Linear Cryptanalysis

Improved Davies’ attack

Outline

– Simply introduce Differential cryptanalysis

– One-round attack

– Full 16-round attack

– Meet-in-the-middle attack

Differential cryptanalysis

Differential cryptanalysis is a chosen plaintext attack that analyses how the differences in two plaintext messages affects the differences between the corresponding ciphertexts.

Assume: attacker has a large number of tuples (x, x^*, y, y^*),
where $x' = x \oplus x^*$ is fixed

It is similar to linear attack.

The main difference from linear cryptanalysis is that differential cryptanalysis involves comparing the x-or of two inputs to the x-or of the corresponding two outputs

Differential cryptanalysis

● The expansion function E and the final permutation function P are easily invertible, so they can essentially be ignored

● we can also ignore the subkey XOR stage of the F-function
Proof: Suppose we take two inputs to the F-function m_1 , m_2 , it is differ by a known amount Δ_I . Consider bit strings message as elements of Z_2^{32}

$$m_2 = m_1 + \Delta_I = m_1 \oplus \Delta_I$$

After inputs XOR with the key bits

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2 = \Delta_I$$

So the two inputs retain their difference even after being mixed with the key bits.

Differential cryptanalysis

Definition 1 The table described is called the pairs XOR distribution table. Each row of the table represents an input XOR value and each column represents an output XOR value. The table entries represent the number of possible pairs with such an input XOR and such an output XOR.(the pair is call differential)

Input	Output XOR															
XOR	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
00_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
02_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
03_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
04_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
05_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
06_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
07_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
08_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
09_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
$0A_x$	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
$0B_x$	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
$0C_x$	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
$0D_x$	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
$0E_x$	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8

Table 1: Part of the pairs XOR distribution table of S_1.

Differential cryptanalysis

Definition 2 Let S'_{iI} be an input XOR to an S-box and S'_{iO} be an output XOR for an S-box. We say S'_{iI} may cause S'_{iO} if there exists an input pair $S_{iI,}$ S^*_{iI} such that $S'_{1I} = S_{iI} \oplus S^*_{iI}$ and

$$S'_{iO} = S_i(S_{iI}) \oplus S_i(S_{iI}^*) = S_{iO} \oplus S^*_{iO}$$

We write $S'_{iI} \rightarrow S'_{iO}$ if this happens.

Definition 3 For the S-box S_i ,define the set of inputs $S_{iI,}$ S^*_{iI} such that $S'_{iI} \rightarrow S'_{iO}$ to be

$$IN_i(S'_{iI} \rightarrow S'_{iO}) = \{S_{iI} \mid S_i(S_{iI}) \oplus S_i(S_{iI}^*) = S'_{iO}\}$$

And define the number of such input to be

$$N(S'_{iI} \rightarrow S'_{iO}) = |IN_i(S'_{iI} \rightarrow S'_{iO})|$$

The probability that $S'_{iI} \rightarrow S'_{iO}$ is

$$P(S'_{iI} \rightarrow S'_{iO}) = N(S'_{iI} \rightarrow S'_{iO}) / 64$$

The 1-Round Attack

Precomputations

Assume input pair $S_{1E} = 08_x$ and $S_{1E}^* = 04_x$ and secret key $S_{1k} = 1A_x$
Tracing through the F-function, we see

$$S_{1I} = S_{1E} \oplus S_{1k} = 08_x \oplus 1A_x = 12_x$$

$$S_{1I}^* = S_{1E}^* \oplus S_{1k} = 04_x \oplus 1A_x = 1E_x$$

Using S-box S_1

$$S_{1O} = S_1(S_{1I}) = S_1(12_x) = A_x$$

$$S_{1O}^* = S_1(S_{1I}^*) = S_1(1E_x) = 7_x$$

Thus

$$S'_{1O} = S_{1O} \oplus S_{1O}^* = A_x \oplus 7_x = D_x$$

The 1-Round Attack

Similar process, we find pair $S_{1E} = 34_x$ and $S_{1E}^* = 38_x$

$S_{1I} = S_{1E} \oplus S_{1k}$
$= 2E_x$

$S_{1I}^* = S_{1E}^* \oplus S_{1k}$
$= 22_x$

$S_{1O} = S_1 (S_{1I})$
$= B_x$

$S_{1O}^* = S_1 (S_{1I}^*)$
$= 1_x$

$S'_{1O} = A_x$

The 1-Round Attack

Suppose we only know that input pair $S_{1E} = 08_x$ and $S_{1E}^* = 04_x$ and $S'_{1O} = D_x$

We want to determine S_{1k} .

We see that $S'_{1E} = S'_{1I} = 0C_x$, regardless of the value of S_{1k}

The number of pairs is $N(0C_x \rightarrow D_x) = 6$ (from XOR distribution table)

Constructing a table of input pairs ordered by the resulting output XOR

Notice that each line represents a set $IN_1(0C_x, S'_{iO})$ where $0C_x \rightarrow S'_{iO}$

The 1-Round Attack

Output XOR (S'_{1O})	Possible Inputs (S_{1I})
3_x	10_x, 14_x, 18_x, $1C_x$, 24_x, 28_x, 31_x, $3D_x$
5_x	0_x, C_x, 15_x, 16_x, 19_x, $1A_x$
6_x	7_x, B_x, 20_x, $2C_x$, 33_x, $3F_x$
9_x	5_x, 9_x, 11_x, $1D_x$, 35_x, 39_x
A_x	22_x, $2E_x$, 30_x, 34_x, 38_x, $3C_x$
B_x	23_x, 27_x, $2B_x$, $2F_x$
C_x	2_x, E_x, 25_x, 29_x, 32_x, $3E_x$
D_x	1_x, D_x, 12_x, $1E_x$, 36_x, $3A_x$
E_x	3_x, 6_x, A_x, F_x, 13_x, 17_x, $1B_x$, $1F_x$, 21_x, 26_x, $2A_x$, $2D_x$, 37_x, $3B_x$
F_x	4_x, 8_x

The 1-Round Attack

Since $S'_{iO} = D_x$, we know that

$$S_{1I}, S^*_{1I} \in \{01_x, 0D_x, 12_x, 1E_x, 36_x, 3A_x\}$$

Moreover, since $S'_{1E} = 0C_x$ we have

$$(S_{1I}, S^*_{1I}) \in \{(01_x, 0D_x), (12_x, 1E_x), (36_x, 3A_x)\}$$

Now

$$S_{1I} = S_{1E} \oplus S_{1k} \rightarrow S_{1k} = S_{1I} \oplus S_{1E}$$

S-box inputs		Possible S_{1K} values	
01_x	$0D_x$	09_x	05_x
12_x	$1E_x$	$1A_x$	16_x
36_x	$2A_x$	$3E_x$	32_x

Possible keys for $0C_x \rightarrow D_x$ input $(S_{1E}, S^*_{1E}) = (08_x, 04_x)$

The 1-Round Attack

Suppose we take $S_{1E} = 38_x$ and $S_{1E}^* = 34_x$ and $S'_{1O} = A_x$

So

$S_{1I}, S^*_{1I} \in \{22_x, 2E_x, 30_x, 34_x, 38_x, 3C_x\}$

Moreover that

$(S_{1I}, S^*_{1I}) \in \{(22_x, 2E_x), (30_x, 34_x), (38_x, 3C_x)\}$

S-box inputs		Possible S_{1K} values	
22_x	$2E_x$	16_x	$1A_x$
30_x	$3C_x$	04_x	08_x
34_x	38_x	00_x	$0C_x$

Possible keys for $0C_x \to A_x$ input $(S_{1E}, S^*_{1E}) = (38_x, 34_x)$.

Unfortunately, $16_x \oplus 1A_x = 0C_x$

So additional input pairs with an XOR of $0C_x$ can not distinguish between these two value

The 1-Round Attack

Suppose we take $S_{1E} = 3B_x$ and $S_{1E}^* = 2B_x$ and $S'_{1O} = A_x$

Input XOR 10_x

Output XOR (S'_{1O})	Possible Inputs (S_{1I})
6_x	$0A_x$, $1A_x$
7_x	08_x, 09_x, $0B_x$, 18_x, 19_x, $1B_x$, 23_x, 24_x, $2C_x$, $2D_x$, 33_x, 34_x, $3C_x$, $3D_x$
9_x	03_x, $0F_x$, 13_x, $1F_x$, $2B_x$, $3B_x$
A_x	01_x, 11_x, 21_x, $2F_x$, 31_x, $3F_x$
B_x	04_x, 05_x, $0C_x$, 14_x, 15_x, $1C_x$, 20_x, 25_x, $2E_x$, 30_x, 35_x, $3E_x$
C_x	27_x, $2A_x$, 37_x, $3A_x$
D_x	00_x, 06_x, 10_x, 16_x, 22_x, 32_x
E_x	02_x, $0D_x$, 12_x, $1D_x$, 28_x, 29_x, 38_x, 39_x
F_x	07_x, $0E_x$, 17_x, $1E_x$, 26_x, 36_x

Possible input values for the input XOR S'_{1I} by the output XOR

The 1-Round Attack

S-box inputs		Possible S_{1K} values	
01_x	11_x	$3A_x$	$2A_x$
21_x	31_x	$1A_x$	$0A_x$
$2F_x$	$3F_x$	14_x	04_x

The Full 16-round DES

The lack of progress in the cryptanalysis of the full DES led many researchers to analyses simplified variants of DES, and in particular variants of DES with fewer than 16 round.

- **Chaum and Evertse :** attack on reduced variants of DES, complexity is 2^{54} for 6 round but this attack is not applicable to variants with eight or more round.

- **Davies:** devised a known plaintext attack whose application to DES reduced to eight rounds. 2^{40} plaintext, the time complexity is 2^{40}
  but this attack is not applicable to the full 16 round DES, since it has to analyze more than the 2^{64} possible plaintext

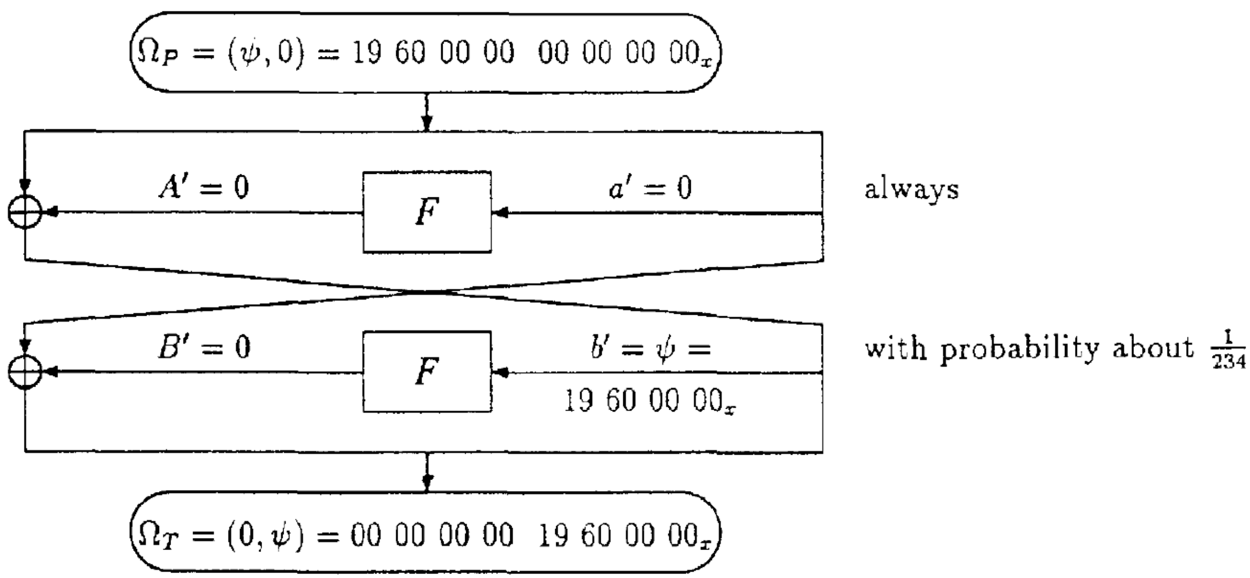
- **Differential cryptanalysis :** it could break variants of DES with up to 15 rounds faster than via exhaustive search
  but for the full 16 round DES the complexity of attack 2^{58} , it is slower than exhaustive search

The Full 16-round DES

The New Attack

- we ignore the initial permutation IP and final permutationIP^{-1} of DES

- the old attack on the 15-round variant of DES was based on the following two round iterative characteristic



The Full 16-round DES

- The 13-round characteristic results from iterating this characteristic six and a half times and probability is about $2^{-47.2}$
- Followed by a 2-round attack on rounds 14 to 15
  2-round attack is input XOR is zero and output XOR is zero
- Any pair of plaintexts which gives rise to the intermediate XORs specified by this characteristic is called a right pair (differential holds)
- The attack tries many pairs of plaintext, and eliminates any pair which is obviously wrong due to its known input and output value.

The Full 16-round DES

Earlier versions of differential cryptanalysis

- each surviving pair suggested several possible values for certain key bits
- right pairs always suggest the correct value for these key bits
  wrong pairs suggest random values
- The actual algorithm is to keep a separate counter for the number of times each value is suggested, and to output the index of the counter with the maximal final value.

New versions of differential cryptanalysis

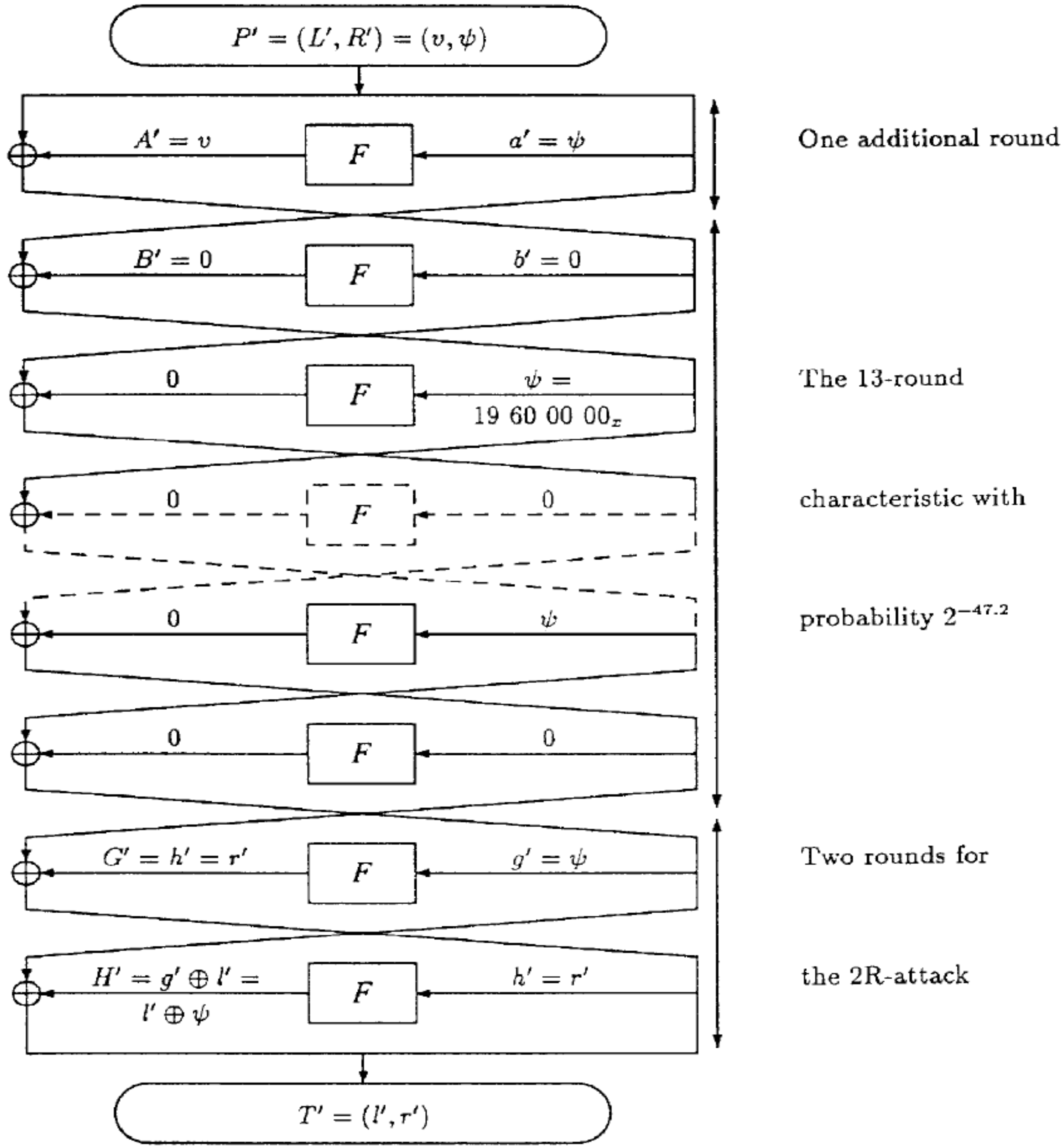
- suggest a list of complete 56-bit keys
- we can immediately test each suggested key via trial encryption without using any counters
- these texts can be carried out in parallel on disconnected processors with very small memories
- algorithm is guaranteed to discover the correct key as soon as the first right pair is encountered

The Full 16-round DES

Obvious way to extend the attack to 15 rounds is to use iterative characteristic in 15 round one more time, but this reduces the probability of the characteristic From $2^{-47.2}$ to $2^{-55.1}$,slower than exhaustive search

The idea of new attack is adds the extra round without reducing the probability at all

Our goal is to generate without loss of probability pairs of plaintexts whose XORed outputs after the first round are the required XORed inputs (ψ, 0) into the 13-round characteristic of rounds 2 to 14.



P' = (L', R') = (v, ψ)
A' = v
F
a' = ψ
One additional round
B' = 0
F
b' = 0
0
F
ψ =
19 60 00 00x
The 13-round
0
F
0
characteristic with
0
F
ψ
probability 2^-47.2
0
F
0
G' = h' = r'
F
g' = ψ
Two rounds for
H' = g' ⊕ l' =
l' ⊕ ψ
F
h' = r'
the 2R-attack
T' = (l', r')

The Full 16-round DES

Let P be an arbitrary 64-bit plaintext, and let $v_0, \ldots, v_{4095}$ be the 2^{12} 32-bit constants which consist of all the possible values at the 12 bit positions which are XORed with the 12 output bits of S1, S2 and S3 after the first round, and 0 elsewhere.

We now define a structure which consists of 2^{13}plaintexts:

$$P_i = P \oplus (v_i, 0) \qquad \bar{P}_i = (P \oplus (v_i, 0)) \oplus (0, v_i) \qquad \text{for } 0 <= I < 2^{12}$$

$$T_i = DES(P_i, k) \qquad \bar{T}_i = DES(\bar{P}_i, k)$$

There are 2^{24} such plaintext pairs, and their XOR is always of the form(v_k, ψ), where each v_k occurs exactly 2^{12} time

The Full 16-round DES

The additional one round output is the desired input XOR(ψ, 0**)**

- The actual processing of the left half of P and of the left half of P XORed with ψ in the first round under the actual key creates a XORed value after the first round which can be non-zero only at the outputs of s1, s2 and s3, this XORed value is one of the v_k
- For exactly 2^{12} of the plaintext pairs, the output XOR of the first F-function is exactly cancelled by XORing it with the left half of the plaintext XOR.
- Thus the output XOR of the first round (after swapping the left and right halves) is the desired input XOR (ψ, 0) into the iterative characteristic.

The Full 16-round DES

Data collection phase

● In any right pair, the output XOR after 16-round should be zero at the outputs of the five S-box S_4……S_8

● sorted ciphertexts and detect all the repeated occurrences of values

● If there has a non-zero ciphertext XOR, the plaintexts is fails, it can not be right pair by definition

● By testing additional S boxes in the first, fifteenth, and sixteenth rounds and eliminating all the pairs whose XOR values are indicated as impossible in the pairs XOR distribution tables of the various S boxes, we can discard about 92.55% of these surviving pairs' leaving only 16*0.0745 = 1.19 pairs per structure as the expected output of the data collection phase

The Full 16-round DES

Data analysis phase

- Try each suggested value of the key

- A key value is suggested when it can create the output XOR values of the last round as well as the expected output XOR of the first round and the fifteenth round for the particular plaintext pairs and ciphertext pairs

- in the first round and in the fifteenth round the input XORs of S_4 and S_5 ….S_8 are always zero

- From key scheduling algorithm, all the 28 bits of the left key are used as inputs to S boxes S_1 , S_2 , S_3 in the first round and fifteenth rounds and S_1 ….S_4 in the sixteenth round
  24 bits of the right key register are used in the sixteenth round

- comparing the output XOR of the last round to its expected value and discarding the ones whose values are not possible

The Full 16-round DES

- comparing the output XOR of the three S boxes in the first round to its expected value

- each structure suggests about 16 choices for the whole key (56 bits)

- each remaining choice of 56 bits key is verified via trial encryption of one of plaintext and comparing the result to the corresponding ciphertext
  if test succeeds, there is a very high probability that this key is the right key

Meet-in-the-Middle Attack on 4-round DES

Short description of meet-in-the-middle attacks

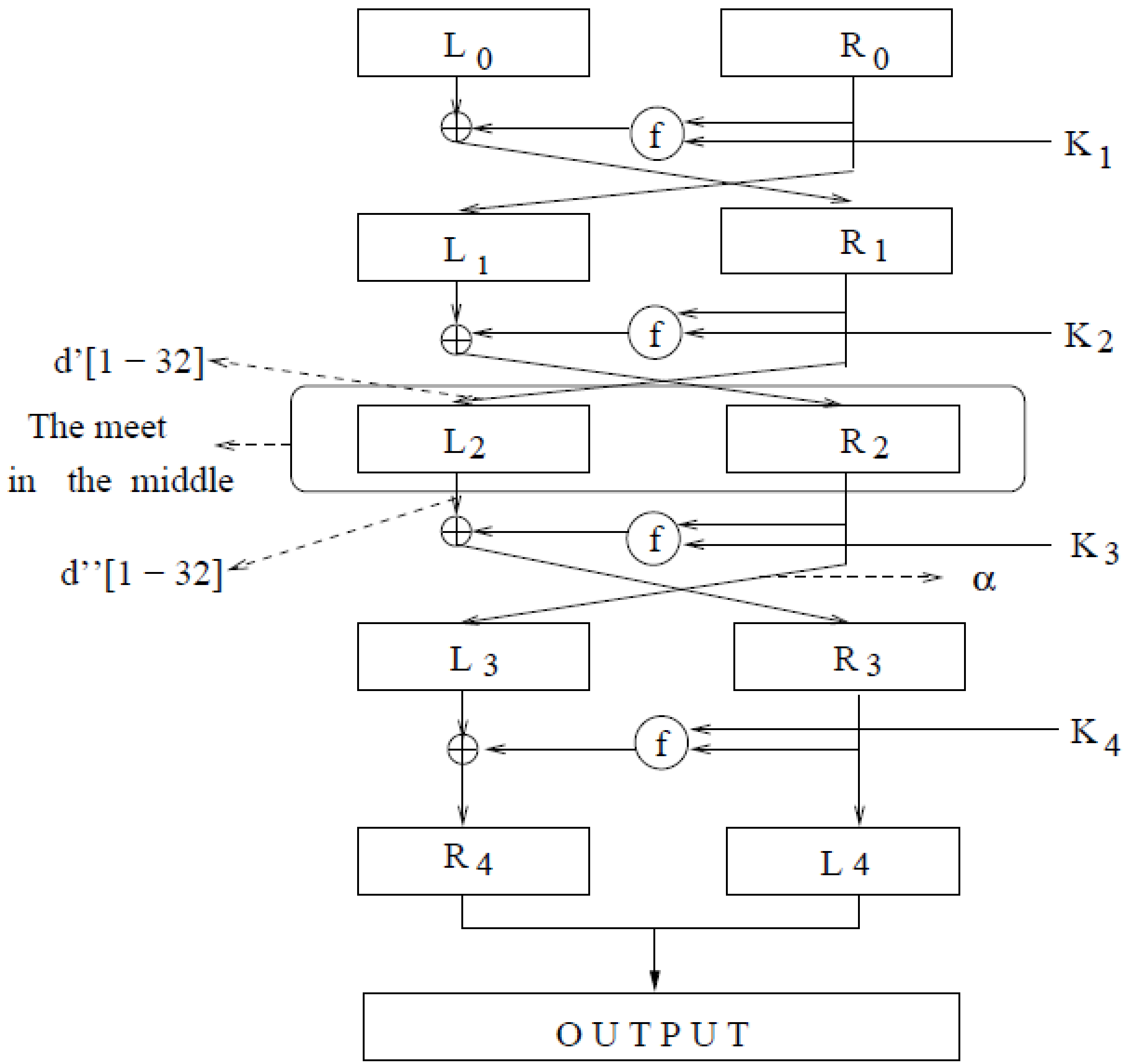
Let M denote the message space and K denote the key space

Suppose that G_k ,H_k : M × K → M are two block cipher, let $F_k = G_k \circ H_k$

The attacker tries to deduce K from a given plaintext ciphertext pair c = F_k(p) by tring to solve

$$G_k(p) = H_k^{-1}(c)$$

Let d’[1-m] = G_k(p) , d’’[1-m] = H_k^{-1}(c),
G_k consists of the first 2 rounds of DES
H_k contain of rounds 3 and 4


L 0
R 0
f
K 1
L 1
R 1
f
K 2
d'[1 − 32]
The meet
in the middle
L 2
R 2
f
K 3
d''[1 − 32]
α
L 3
R 3
f
K 4
R 4
L 4
OUTPUT

Meet-in-the-Middle Attack on 4-round DES

Consider d’[9-12] and d’’[9-12], it is sufficient to guess only 37key bits.

If d’[9-12] != d’’[9-12] , then the key guess cannot be correct and discarded

The main observation is the fact that the values of d’[9-12] and d’’[9-12] can be computed by guessing less key bits in exchange for guessing internal bits

$d'[9\text{-}12] = L_0[9\text{-}12] \oplus S_3[EP(R_0)[13\text{-}18] \oplus K_1[13\text{-}18]]$

$d''[9\text{-}12] = L_4[9\text{-}12] \oplus S_3[EP(L_3)[13\text{-}18] \oplus K_3[13\text{-}18]]$

Let $L_3 = [\alpha_1 \ldots\ldots \alpha_{32}]$, then $EP(L_3)[13\text{-}18] = [\alpha_{17}\alpha_1\alpha_{15}\alpha_{23}\alpha_{26}\alpha_5]$

Consider $\alpha_{17.}$ it could be to guess all the 37 key bits suggested, besides the 6 bits which compose $K_4[25\text{-}30]$.

For each guess of the 31 key bits, the attacker tries the two possibilities of α_{17}

If for both values the equality d’[9-12] = d’’[9-12] is not achieved
Then the guess of the 31 bits is necessarily wrong

Meet-in-the-Middle Attack on 4-round DES

Kinds of Meet-in-the-middle attack

One known plaintext

Multiple known plaintext

Chosen ciphertexts

Quiz

1. List three kinds of DES attack
2. List the main steps in 1-round attack
3. If the objective is to save memory, which place are shown additional new round when we do new attack in full 16-round attack
4. What the output of the additional one round?
5. When will the key guess be correct, given the values of d’[9-12] and d’’[9-12]?