Improved Meet-in-the-Middle Attacks on Reduced-Round DES

Halil İbrahim Kaplan

2021

TÜBİTAK

BİLGEM

Overview

- Description of DES
- Meet-in-the-Middle Attack on 4-Round DES
- Attack on 5-Round DES
- Attack on 6-Round DES

Description of DES

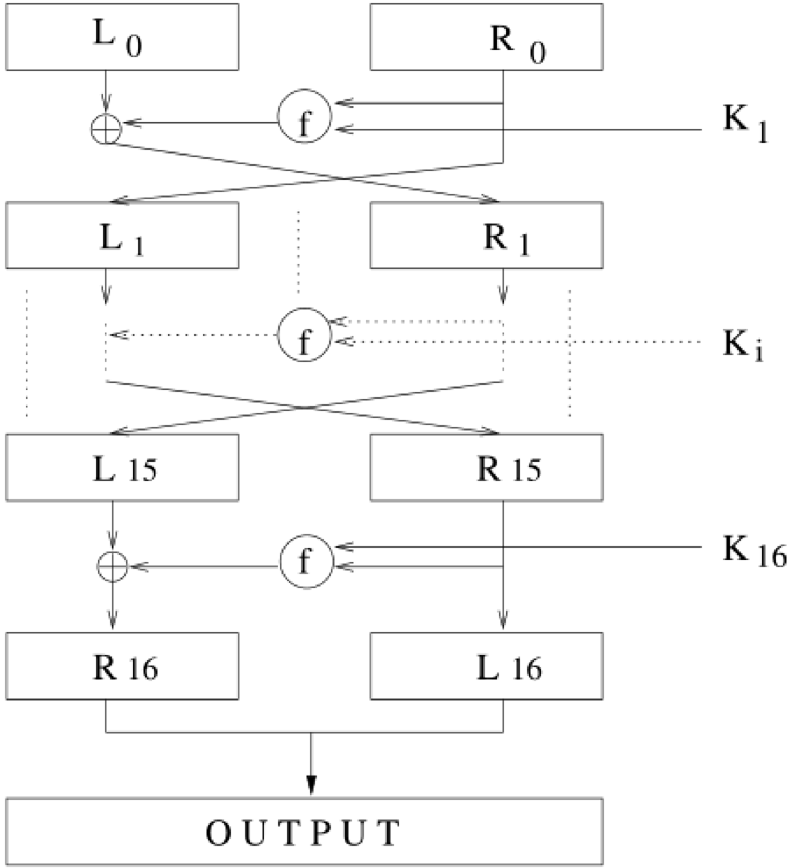


Fig. 1. General structure of the Data Encryption Standard

K_i = i-th subkey

1	2	3	...	...	...	...	...	55	56

Y [a–b] = bits a, . . . , b of Y .

Description of DES

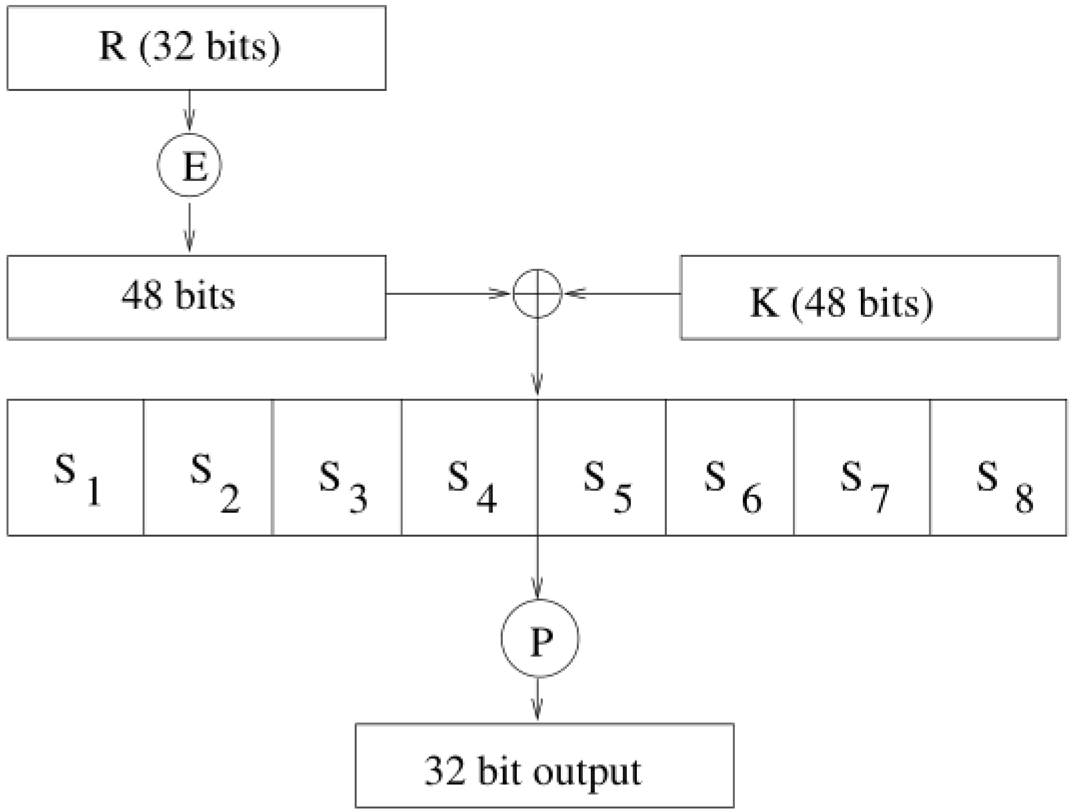


Fig. 2. *F*-function of DES

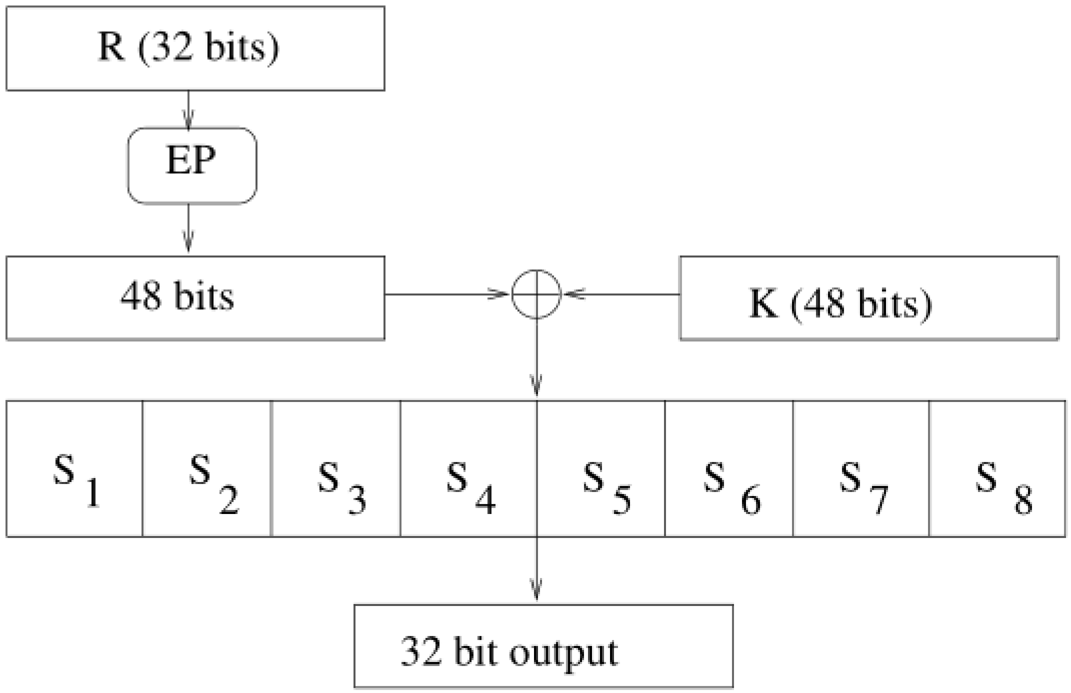


Fig. 3. An alternative description of DES *F*-function

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

Suppose that $G_K, H_K : \mathrm{M} \times \mathrm{K} \rightarrow \mathrm{M}$ are two block ciphers and let $F_K = H_K \circ G_K$.

Attacker tries to deduce K from a given plaintext ciphertext pair c = F_K(p) by trying to solve

$$G_K(\mathrm{p}) = H_K^{-1}(\mathrm{c})$$

In some of the cases, the equation is not tested for all the bits of the intermediate encryption value, but rather to only some of them.

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

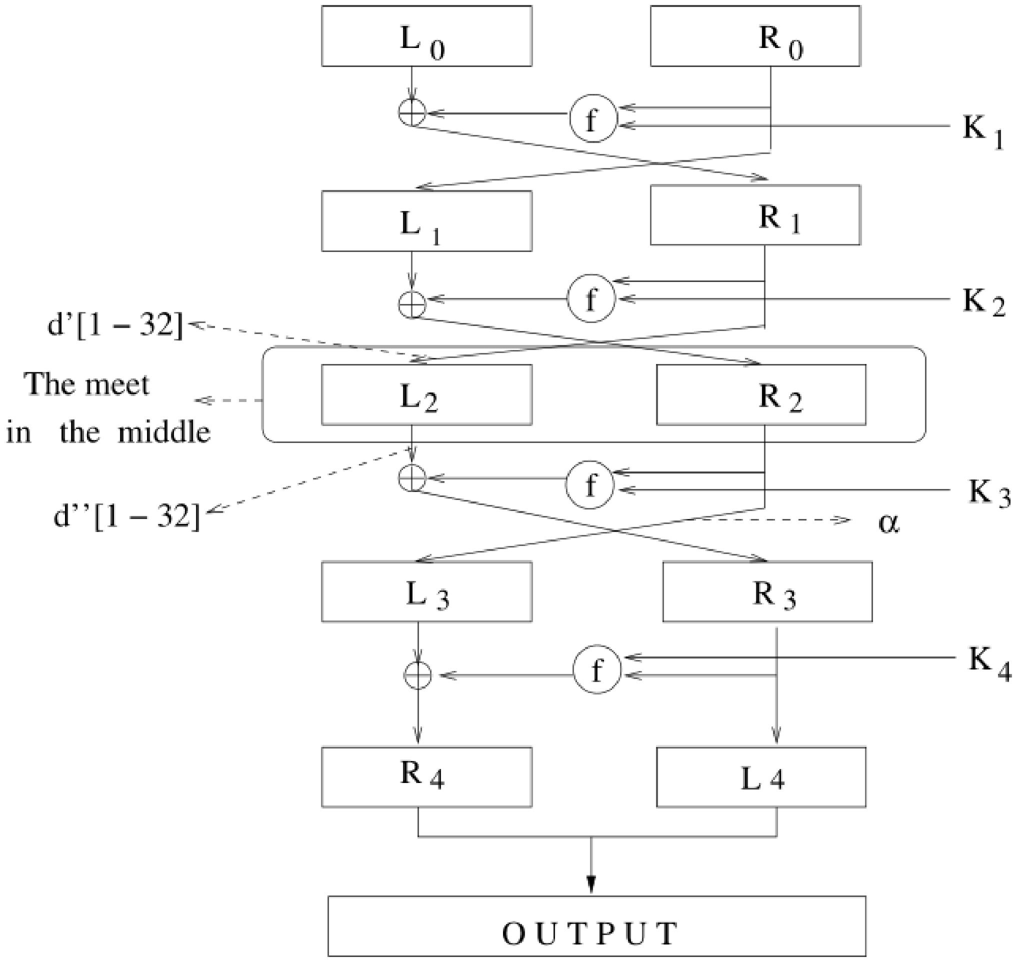


Fig. 4. 4-Round DES

It was observed in [3] that in order to compute d′[9–12] and d″[9–12], it is sufficient to guess only 37 key bits.

$$d'[9\text{–}12] \neq d''[9\text{–}12] \implies \text{Key guess is not correct}$$

IDEA :

d′[9–12] and d″[9–12] can be computed by guessing less key bits in exchange for guessing internal bits.

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

Consider $d'[9\text{–}12]$, this value is equal to:

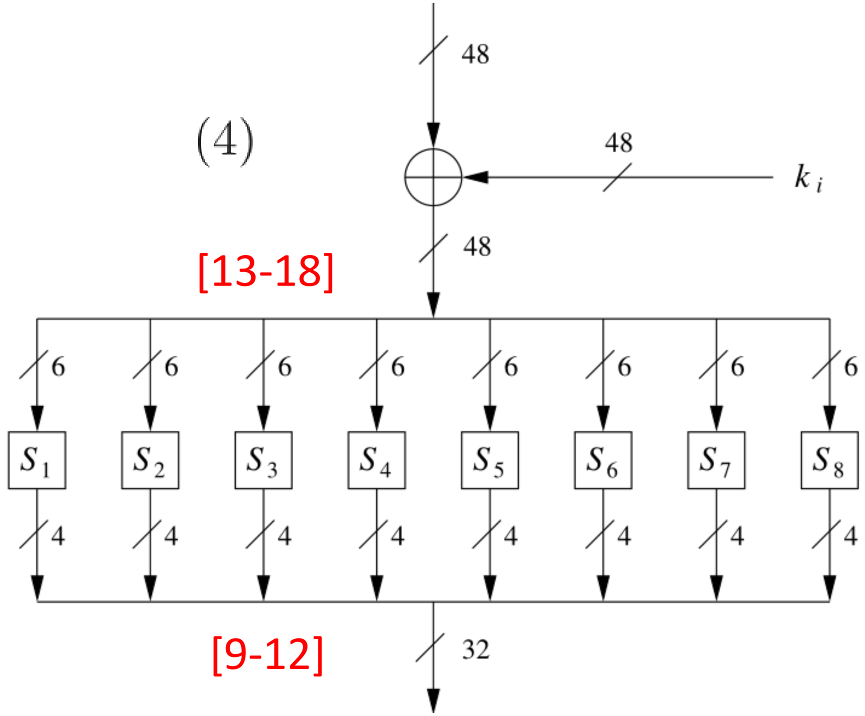
$$d'[9\text{–}12] = L_0[9\text{–}12] \oplus S_3[EP(R_0)[13\text{–}18] \oplus K_1[13\text{–}18]] \tag{2}$$

and $d''[9\text{–}12]$ is equal to

$$d''[9\text{–}12] = L_4[9\text{–}12] \oplus S_3[EP(L_3)[13\text{–}18] \oplus K_3[13\text{–}18]]. \tag{3}$$

Let $L_3 = [\alpha_1\text{–}\alpha_{32}]$, then

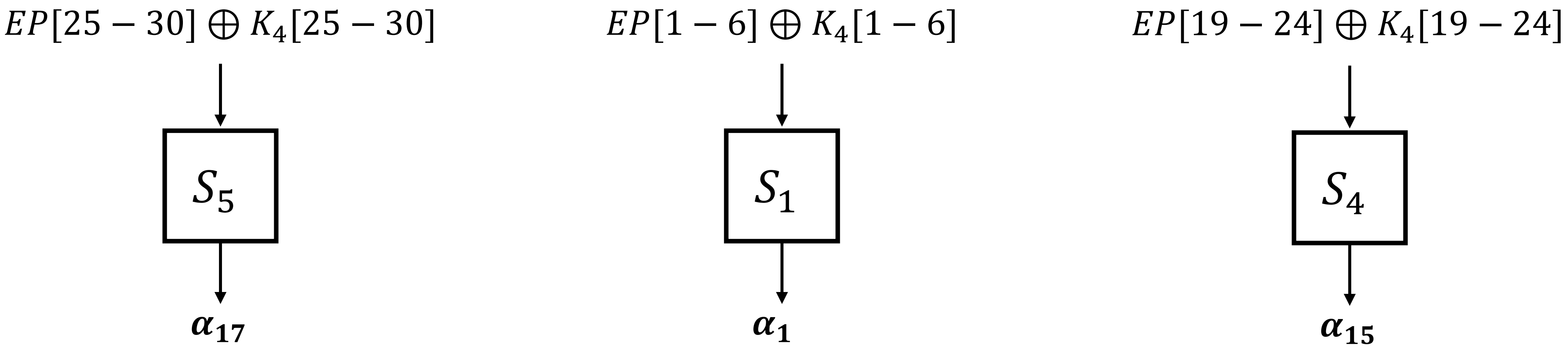
$$EP(L_3)[13\text{–}18] = [\alpha_{17}\alpha_1\alpha_{15}\alpha_{23}\alpha_{26}\alpha_5]. \tag{4}$$



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

If we guess K_1[13–18] and K_3[13–18], the only remaining unknowns in the computation of d″[9–12] are

$$[\boldsymbol{\alpha_{17}\ \alpha_1\ \alpha_{15}\ \alpha_{23}\ \alpha_{26}\ \alpha_5}]$$



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

Table 2. Key bits determining the 'middle' bits of 4-round DES

Round/S-box	Key bits	Bit determined	Bits appearing once †
1/3	5, 9, 13, 20, 24, 27		24
1/8	30, 33, 37, 43, 47, 51	α_{17}	30, 33, 37, 43, 47, 53
3/3	2, 8, 12, 16, 23, 27		
4/1	2, 7, 11, 17, 20, 23	α_1	7, 11, 17
4/2	6, 9, 12, 16, 21, 27	α_5	6, 21
4/4	5, 8, 13, 19, 22, 26	α_{15}	19, 22, 26
4/6	29, 36, 39, 46, 51, 54	α_{23}	29, 36, 39, 46, 51, 54
4/7	31, 34, 40, 45, 50, 55	α_{26}	31, 34, 40, 45, 50, 55
Bits of K not affecting (1)	1,3,4,10,14,15,18,25,28,32,38,41,42,44,48,49,52,56		

† — These bits appear only once in computing d' and d''.

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

If we guess $K_1[13–18]$ and $K_3[13–18]$, the only remaining unknowns in the computation of d″[9–12] are

$$[\boldsymbol{\alpha_{17}\ \alpha_1\ \alpha_{15}\ \alpha_{23}\ \alpha_{26}\ \alpha_5}]$$

HERE WE HAVE 2 OPTIONS

We can guess 37 key bits

OR

We can directly guess one or more bits from remaining unknowns

Lets say we are guessing $\boldsymbol{\alpha_{17}}$

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

For each guess of 31 bits

try 2 possibilities of α_{17}

If $d'[9–12] \neq d''[9–12]$ for all possibilty of α_{17} , **then** guess of 31 bits is wrong.

If $d'[9–12] = d''[9–12]$ at least one possibilty of α_{17} , **then** guess of 31 bits may be correct.

Probability that a wrong 31-bit key guess has at least one α_{17} for which the equality is satisfied = $1 - (\frac{15}{16})^2 \approx 1/8$.

So,

With guessing 31 bits and trying 2 possibilities of α_{17} , we can reduce the possible key candidates to $2^{31} * 2^{-3} = 2^{28}$

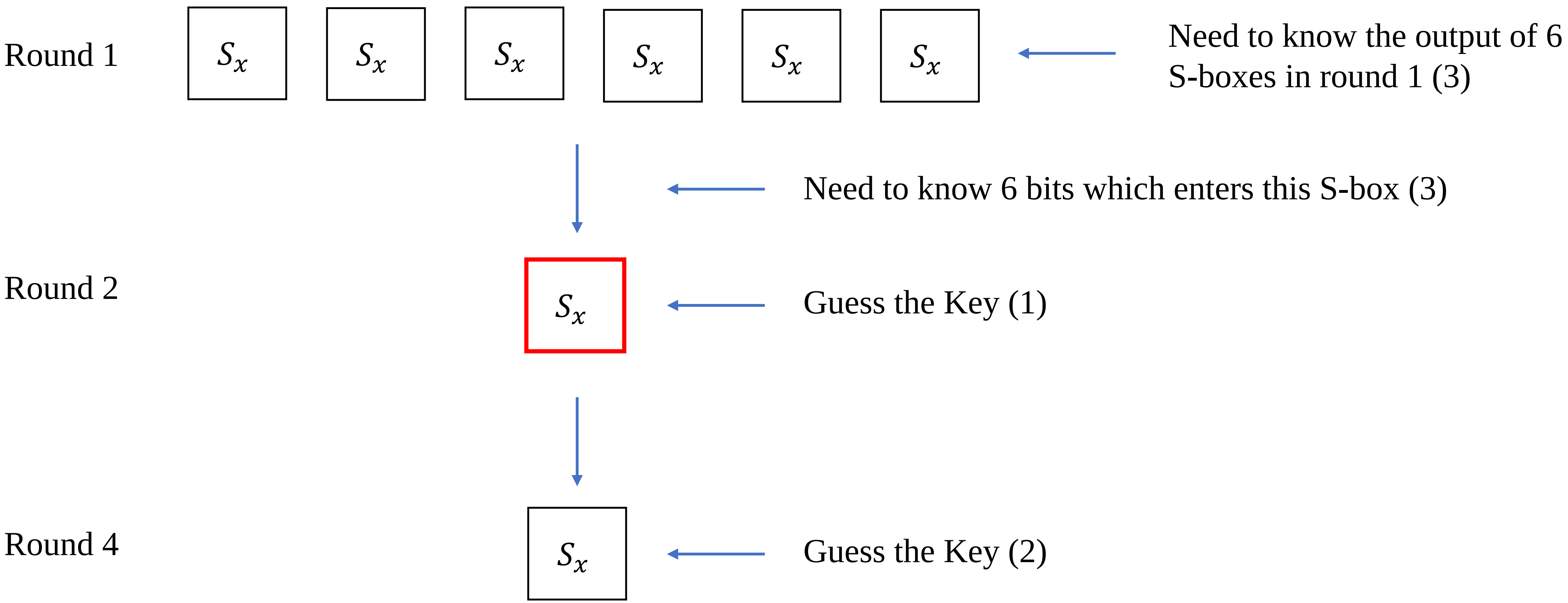
Meet-in-the-Middle Attack on 4-Round DES

Guess more α_i values $\Longrightarrow$ Reduces number of possible keys $\Longrightarrow$ Increase the probability that a wrong key remains

# of guessed bits	Probability
2	$1-(\frac{15}{16})^4 \approx 2^{-2.1}$
3	$1-(\frac{15}{16})^8 \approx 2^{-1.3}$
4	$1-(\frac{15}{16})^{16} \approx 2^{-0.6}$

Using One Known Plaintext:

Attacking S_x in round 2 means that :



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

Using One Known Plaintext:

For example, performing a meet-in-the-middle on S3 of round 2 :

Guess

K_1[1–12], K_1[19–24], K_2[13–18], K_4[13–18] (a total of 19 bits),

Guess

3 intermediate encryption values (α_{17}, α_{23}, α_{26}).

Apply attack for the 2^{19} possible values for the 19bit key,

$2^{19} * 2^{-1.3} = 2^{17.7}$ key values remain.

Round	S-box	Number of Guessed Key Bits	Number of Guessed Intermediate Bits	Number of Remaining Key Guess
2	$S3$	19	3	$2^{19} \cdot 2^{-1.3} = 2^{17.7}$
3	$S2$	+3	4	$2^{17.7} \cdot 2^{3} \cdot 2^{-0.6} = 2^{20.1}$
2	$S1$	+2	4	$2^{20.1} \cdot 2^{2} \cdot 2^{-0.6} = 2^{21.5}$
3	$S4$	+3	3	$2^{21.5} \cdot 2^{3} \cdot 2^{-1.3} = 2^{23.2}$
$2^{\dagger}$	$S4$	+1	3	$2^{23.2} \cdot 2^{1} \cdot 2^{-1.3} = 2^{22.9}$
3	$S3$	-	3	$2^{22.9} \cdot 2^{-1.3} = 2^{21.6}$
2	$S2$	-	4	$2^{21.6} \cdot 2^{-0.6} = 2^{21.0}$
3	$S1$	-	4	$2^{21.0} \cdot 2^{-0.6} = 2^{20.4}$
2	$S8$	+9	2 $(-2)^{\ddagger}$	$2^{20.4} \cdot 2^{9} \cdot 2^{-4} = 2^{25.4}$
3	$S5$	+5	1 $(-5)^{\ddagger}$	$2^{25.4} \cdot 2^{5} \cdot 2^{-8} = 2^{22.4}$
3	$S6$	+4	2 $(-5)^{\ddagger}$	$2^{22.4} \cdot 2^{4} \cdot 2^{-7} = 2^{19.4}$
2	$S7$	+4	1 $(-4)^{\ddagger}$	$2^{19.4} \cdot 2^{4} \cdot 2^{-7} = 2^{16.4}$
3	$S7$	+3	2 $(-5)^{\ddagger}$	$2^{16.4} \cdot 2^{3} \cdot 2^{-7} = 2^{12.4}$
3	$S8$	+2	1 $(-9)^{\ddagger}$	$2^{12.4} \cdot 2^{2} \cdot 2^{-12} = 2^{2.4}$

Exhaustively search the remaining $2^{3.4}$ keys.

† — At this point the entire half of the key is known.
‡ — The $(-i)$ means that there i bits that were earlier guessed are now known (and can be used to discard wrong guesses).

$2^{-2} * 2^{-2.1} \approx 2^{-4}$

$2^{-5} * 2^{-3} \approx 2^{-8}$

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

Using Multiple Known Plaintexts:

Guess

3 intermediate bits,

With first plaintext/ciphertext pair

Reduce the number of possible keys to $2^{19} * 2^{-1.3} = 2^{17.7}$

Repeat the analysis with the next plaintext/ciphertext pair.

Probability that a key remains after each iteration of the analysis is $1 - (\frac{15}{16})^8 \approx 2^{-1.3} \approx 0.4$

$$t \geq 15 \quad \Longrightarrow \quad 2^{19} * (0.4)^t < 1$$

Thus, after 15 plaintext/ciphertext pairs, we expect to have only the right value for 19 key bits

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

Using chosen Ciphertexts:

IDEA: Choose ciphertexts so that intermediate encryption bits which are guessed same for all ciphertexts.

Guess the 19 key bits

Apply attack 1 time

For the next Attacks

For each key candidate which is not discarded,

Test only with the intermediate encryption values which satisfied the meet-in-the-middle condition earlier.

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

Using chosen Ciphertexts:

For a given key,

probabilty to be discarded with first P/C = $1 - 2^{-1.3} \approx 1 - (0.4) = 0.6$

Attack on 5-Round DES

$G_K = Round\ 1 \ \ \& \ \ Round\ 2$

$H_K = Round\ 3 \ \ \& \ \ Round\ 4 \ \ \& \ \ Round\ 5$

$G_K \text{o} H_K = 5 \text{ Round DES}$

In order to compute d′[41–44] and d″ [41–44], it is sufficient to guess only 47 key bits.

$$d'[41\text{–}44] = R_0[9\text{–}12] \oplus S_3[EP(R_1)[13\text{–}18] \oplus K_2[13\text{–}18]]$$

$$d''[41\text{–}44] = L_5[9\text{–}12] \oplus S_3[EP(L_4)[13\text{–}18] \oplus K_4[13\text{–}18]].$$

Attack on 5-Round DES

Let $R_1 = [\beta_1\text{–}\beta_{32}]$, $L_4 = [\gamma_1\text{–}\gamma_{32}]$. Then,

$$EP(R_1)[13\text{–}18] = [\beta_{17}\beta_1\beta_{15}\beta_{23}\beta_{26}\beta_5],$$

$$EP(L_4)[13\text{–}18] = [\gamma_{17}\gamma_1\gamma_{15}\gamma_{23}\gamma_{26}\gamma_5].$$

If we guess K_2[13–18] and K_4[13–18], the only remaining unknowns in the computation of d′[41–44] and d″ [41–44] are

$$[\boldsymbol{\beta_{17}\ \beta_1\ \beta_{15}\ \beta_{23}\ \beta_{26}\ \beta_5}] \qquad [\boldsymbol{\gamma_{17}\ \gamma_1\ \gamma_{15}\ \gamma_{23}\ \gamma_{26}\ \gamma_5}]$$

Attack on 5-Round DES

If we guess $K_2[13–18]$ and $K_4[13–18]$, the only remaining unknowns in the computation of d′[41–44] and d″ [41–44] are

$$[\boldsymbol{\beta_{17}\ \beta_1\ \beta_{15}\ \beta_{23}\ \beta_{26}\ \beta_5}] \qquad [\boldsymbol{\gamma_{17}\ \gamma_1\ \gamma_{15}\ \gamma_{23}\ \gamma_{26}\ \gamma_5}]$$

HERE WE HAVE 2 OPTIONS

We can guess 47 key bits

OR

We can directly guess one or more bits from remaining unknowns

Lets say we are guessing β_1

Attack on 5-Round DES

Table 3. Key bits determining the 'middle' bits of 5-round DES

Round/S-box	Key bits	Bit determined	Bits appearing once †
1/1	2,6,12,15,18,25	β_1	2, 12
1/2	1,4,7,11,16,22	β_5	16
1/4	3,8,14,17,21,28	β_{15}	3, 17
1/5	32,38,42,48,53,56	β_{17}	
1/6	31,34,41,46,49,52	β_{23}	34, 46
1/7	29,35,40,45,50,54	β_{26}	40, 50, 54
2/3	6,10,14,21,25,28		
4/3	1,4,10,14,18,25		
5/1	4,9,13,19,22,25	γ_1	9, 13, 19
5/2	1,8,11,14,18,23	γ_5	23
5/4	7,10,15,21,24,28	γ_{15}	24
5/5	32,35,39,45,49,55	γ_{17}	39,55
5/6	31,38,41,48,53,56	γ_{23}	
5/7	29,33,36,42,47,52	γ_{26}	33, 36, 47
Bits of K not affecting (1)	5,20,26,27,30,37,43,44,51		

† — These bits appear only once in computing d' and d''.

Attack on 5-Round DES

For each guess of 45 bits

try 2 possibilities of β_1

If d′[41–44] ≠ d″ [41–44] for 2 posssibilty, **then** guess of 45 bits is wrong.

If d′[41–44] = d″[41–44] at least one possibilty of α_{17} , **then** guess of 31 bits may be correct.

Probability that a wrong 45-bit key guess has at least one β_1 for which the equality is satisfied = $1 - (\frac{15}{16})^2 \approx 1/8$.

So,

With guessing 45 bits and trying 2 possibilities of β_1 , we can reduce the possible key candidates to $2^{45} * 2^{-3} = 2^{42}$

More Efficient Attack:

Table 3. Key bits determining the 'middle' bits of 5-round DES

Round/S-box	Key bits	Bit determined	Bits appearing once [†]
1/1	2,6,12,15,18,25	β_1	2, 12
1/2	1,4,7,11,16,22	β_5	16
1/4	3,8,14,17,21,28	β_{15}	3, 17
1/5	$\boxed{32,38,42,48,53,56}$	$\boxed{\beta_{17}}$	
1/6	31,34,41,46,49,52	β_{23}	34, 46
1/7	29,35,40,45,50,54	β_{26}	40, 50, 54
2/3	6,10,14,21,25,28		
4/3	1,4,10,14,18,25		
5/1	4,9,13,19,22,25	γ_1	9, 13, 19
5/2	1,8,11,14,18,23	γ_5	23
5/4	7,10,15,21,24,28	γ_{15}	24
5/5	32,35,39,45,49,55	γ_{17}	39,55
5/6	$\boxed{31,38,41,48,53,56}$	$\boxed{\gamma_{23}}$	
5/7	29,33,36,42,47,52	γ_{26}	33, 36, 47
Bits of K not affecting (1)	5,20,26,27,30,37,43,44,51		

† — These bits appear only once in computing d' and d''.

$$\text{To determine } \beta_{17} \text{ and } \gamma_{23}$$
$$\text{it is sufficient to guess only bits}$$
$$\underbrace{31,32,38,41,42,48,53,56}_{8}$$

More Efficient Attack:

Guess values of $\beta_{23}\ \beta_{26}\ \gamma_{17}\ \gamma_{26}$

8 + 24 = 32 bits remains for determining values of d′[41–44] and d′′ [41–44]

Probability that a key remains after each iteration of the analysis is $2^{-0.6} \approx 0.65$

$$2^{32} * (0.65)^t < 1 \implies t \geq 51$$

Thus,

With 51 known plaintext, we can obtain 32 bits of the key.

Attack on 6-Round DES

$$G_K = Round\ 1 \quad \& \quad Round\ 2 \quad \& \quad Round\ 3$$

$$H_K = Round\ 4 \quad \& \quad Round\ 5 \quad \& \quad Round\ 6$$

$$G_K \mathrm{o} H_K = 6 \text{ Round DES}$$

In order to compute d′[5–8] and d″ [5–8], it is sufficient to guess 54 key bits.

$$d'[5\text{–}8] = R_0[5\text{–}8] \oplus S_2[EP(R_1)[7\text{–}12] \oplus K_2[7\text{–}12]]$$

$$d''[5\text{–}8] = R_6[5\text{–}8] \oplus S_2[EP(L_4)[7\text{–}12] \oplus K_4[7\text{–}12]] \oplus S_2[EP(L_6)[7\text{–}12] \oplus K_6[7\text{–}12]].$$

$$EP(R_1)[7\text{–}12] = [\beta_{21}\beta_{29}\beta_{12}\beta_{28}\beta_{17}\beta_1],$$

$$EP(L_4)[7\text{–}12] = [\gamma_{21}\gamma_{29}\gamma_{12}\gamma_{28}\gamma_{17}\gamma_1].$$

If we guess $K_2[7\text{–}12]$, $K_4[7\text{–}12]$ and $K_6[7\text{–}12]$, the only remaining unknowns in the computation of d′[5–8] and d″ [5–8] are

$$[\boldsymbol{\beta_{21}\ \beta_{29}\ \beta_{12}\ \beta_{28}\ \beta_{17}\ \beta_1}] \qquad [\boldsymbol{\gamma_{21}\ \gamma_{29}\ \gamma_{12}\ \gamma_{28}\ \gamma_{17}\ \gamma_1}]$$

<u>HERE WE HAVE 2 OPTIONS</u>

We can guess 54 key bits

<u>OR</u>

We can directly guess one or more bits from remaining unknowns

Lets say we are guessing γ_1

Table 4. Key bits determining the 'middle' bits of 6-round DES

Round/S-box	Key bits	Bit determined	Bits appearing once †
1/1	2,6,12,15,18,25	β_1	
1/3	5,9,13,20,24,27	β_{12}	
1/5	32,38,42,48,53,56	β_{17}	
1/6	31,34,41,46,49,52	β_{21}	
1/7	29,35,40,45,50,54	β_{28}	
1/8	30,33,37,43,47,51	β_{29}	
2/2	2,5,8,12,17,23		
4/2	6,9,12,16,21,27		
5/1	4,9,13,19,22,25	γ_1	4, 19
5/3	3,6,12,16,20,27	γ_{12}	
5/5	32,35,39,45,49,55	γ_{17}	
5/6	31,38,41,48,53,56	γ_{21}	
5/7	29,33,36,42,47,52	γ_{28}	36
5/8	30,37,40,44,50,54	γ_{29}	
There are no key bits of round 6 that appear only once in computing d' and d''.			
Bits of K not affecting (1)	7,28		

† — These bits appear only once in computing d' and d''.

Attack on 6-Round DES

For each guess of 52 bits

try 2 possibilities of γ_1

If d′[5-8] ≠ d″ [5–8] for 2 posssibilty, **then** guess of 52 bits is wrong.

Attacker can reduce the # of possible keys to $2^{52} * 2^{-3} = 2^{49}$ with trying 2 possibilties of γ_1

References

1. Chaum, D., Evertse, J.-H.: Cryptanalysis of DES with a Reduced Number of Rounds: Sequences of Linear Factors in Block Ciphers. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 192–211. Springer, Heidelberg (1986)

2. Dunkelman O., Sekar G., Preneel B. (2007) Improved Meet-in-the-Middle Attacks on Reduced-Round DES. In: Srinathan K., Rangan C.P., Yung M. (eds) Progress in Cryptology – INDOCRYPT 2007. INDOCRYPT 2007. Lecture Notes in Computer Science, vol 4859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77026-8_8