Differential Cryptanalysis and the Theory of S-Box

Exam presentation of Cryptography

Chun TIAN

chun.tian@studio.unibo.it

Outline

- History and Backgrounds
- Differential Cryptanalysis: the Idea
- Differential Cryptanalysis on DES variants
- Design Criteria of DES S-Boxes
- S-Boxes as Boolean functions

Five Maxims in Cryptography

- One should not underrate the adversary.
- Only a cryptanalyst, if anybody, can judge the security of a cryptosystem.
- In judging the encryption security of a class of methods, one has to take into account that the adversary knows the class of methods.
- Superficial complications can be illusory, for they can provide the cryptographer with a false sense of security.
- In judging the encryption security of a class of methods, cryptographic faults and other infringements of security discipline are to be taken into account.

History

- 1949: C. E. Shannon, “Communication Theory of Secrecy Systems”
- 1973: H. Feistel, “Cryptography and data security” (Lucifer)
- 1977: National Bureau of Standards, “Data Encryption Standard” (FIPS 46)
- 1991: E. Biham and A. Shamir. “Differential Cryptanalysis of DES-like Cryptosystems”
- 1992: E. Biham and A. Shamir. “Differential Cryptanalysis of the Full 16-round DES”
- 1994: D. Coopersmith. “The Data Encryption Standard (DES) and its strength against attacks”
- 1994: M. Matsui. “Linear Cryptanalysis Method for DES Cipher”

Differential Cryptanalysis: the Idea

- One-time pad: perfect secrecy

  $c = m \oplus k$
- What happens if we use the key twice?

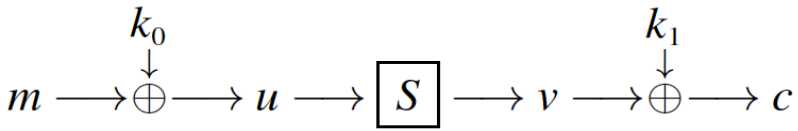
  $c_0 \oplus c_1 = (m_0 \oplus k) \oplus (m_1 \oplus k) = m_0 \oplus m_1$
- While we might not get much information from considering a single message and ciphertext, we might gain much more by considering pairs of messages and ciphertext.

CipherOne

Four-bit block cipher with an eight-bit key and it uses a four-bit look-up box S[·]

$$c = S[m \oplus k_0] \oplus k_1$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b

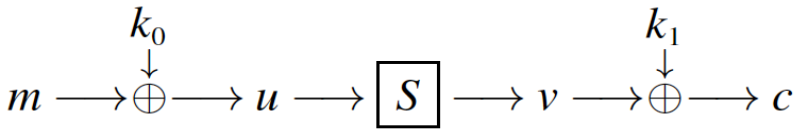


Differential Behavior

- $u_0 \oplus u_1 = (m_0 \oplus k_0) \oplus (m_1 \oplus k_0) = m_0 \oplus m_1$

$$c = S[m \oplus k_0] \oplus k_1$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



Attack CipherOne

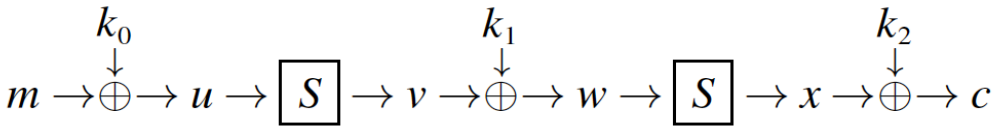
1. Given two message-ciphertext pairs (m_0,c_0) and (m_1,c_1), compute the value of $u_0 \oplus u_1$, as $u_0 \oplus u_1 = m_0 \oplus m_1$;
2. Guess a value t for secret key k_1 and compute the values of v_0 and v_1 directly from c_0 and c_1, as $v_0 = t \oplus c_0$ and $v_1 = t \oplus c_1$;
3. Compute $S^{-1}[v_0]$ and $S^{-1}[v_1]$;
4. If $u0 \oplus u1 = S^{-1}[v0] \oplus S^{-1}[v1]$, then t is noted as a candidate the the secret key k_1; otherwise guess another t' and go back to step 2.
5. If more than one candidate for the key k_1 remains, the attack can be repeated on other messages and ciphertexts.
6. Once k_1 is known, using any single message-ciphertext pair, we can compute out k_0, because $k_0 = m \oplus u = m \oplus S^{-1}[k_1 \oplus c]$

CipherTwo

Four-bit block cipher with an 12-bit key

$$c = S[S[m \oplus k_0] \oplus k_1] \oplus k_2$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



Difference Distribution of S-Box

S-box is non-linear with respect to exclusive-or:

$u_0 \oplus u_1 \nRightarrow S[u_0] \oplus S[u_1]$

But, when $j = i \oplus f$,

$\Pr\{ S[i] \oplus S[j] = d \} = 10/16$

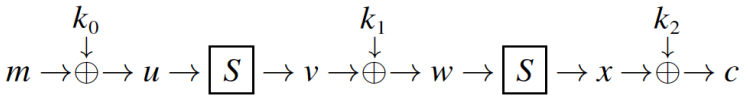
i	j	$S[i]$	$S[j]$	$S[i] \oplus S[j]$
0	f	6	b	d
1	e	4	9	d
2	d	c	a	6
3	c	5	8	d
4	b	0	d	d
5	a	7	3	4
6	9	2	f	d
7	8	e	1	f
8	7	1	e	f
9	6	f	2	d
a	5	3	7	4
b	4	d	0	d
c	3	8	5	d
d	2	a	c	6
e	1	9	4	d
f	0	b	6	d

Attack CipherTwo

1. Pick 16 random message m_0 and set $m_1 = m_0 \oplus f$. We can immediately see that $u_0 \oplus u_1 = m_0 \oplus m_1 = f$;
2. Keep a series of counters $T_0 \ldots T_{15}$ for each possible value of k_2, which are initialized to 0;
3. For each m_0, run through all possible value i of k_2 and if we get $v_0 \oplus v_1 = d$ then increment the counter T_i by 1;
4. When T_i is about 10, the correspond value i is a candidate value of k_2;
5. Once k_2 is known, for each message-ciphertext pair, we can compute $w = S^{-1}[c \oplus k_2]$. Now the rest of cipher is just a CipherOne.

$$c = S[S[m \oplus k_0] \oplus k_1] \oplus k_2$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b

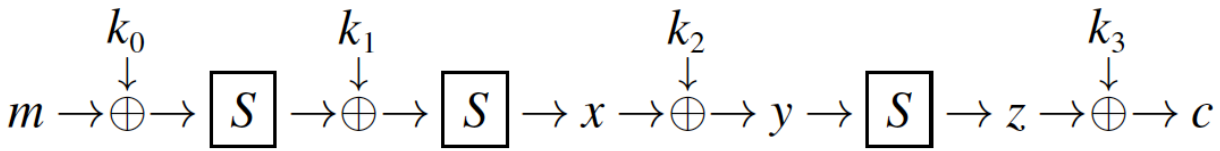


CipherThree

Four-bit block cipher with an 16-bit key

$$c = S[S[S[m \oplus k_0] \oplus k_1] \oplus k_2] \oplus k_3$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



Difference Distribution Table

There is a row for each input difference d_{in} and the frequency with which a given output difference d_{out} occurs is given across the row. The entry (d_{in}; d_{out}) divided by 16 gives the probability that a difference d_{in} gives difference d_{out} when taken over all possible pairs with difference d_{in}.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Characteristic

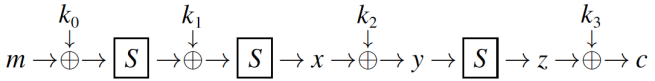
- A pair (α; β) for which two inputs with difference lead to two outputs with difference is called a (differential) characteristic across the operation S[]. It will be denoted by $\alpha \longrightarrow^{S} \beta$.
- A characteristic has a probability associated with it;
- $Pr\{ f \longrightarrow^{S} d \} = 10/16$
- $Pr\{ d \longrightarrow^{S} c \} = 6/16$
- $Pr\{ f \longrightarrow^{S} d \longrightarrow^{S} c \} = 10/16 * 6/16 = 15/64$ (assuming that these characteristics are independent).

Attack CipherThree

1. Pick 16 random message m_0 and set $m_1 = m_0 \oplus f$. We can immediately see that $u_0 \oplus u_1 = m_0 \oplus m_1 = f$;
2. Keep a series of counters $T_0 \ldots T_{64}$ for each possible value of k_3, which are initialized to 0;
3. For each m_0, run through all possible value i of k_3 and if we get $x_0 \oplus x_1 = c$ then increment the counter T_i by 1;
4. When T_i is about 15/4 (= 3 or 4), the correspond value i is a candidate value of k_3;
5. Once k_3 is known, for each message-ciphertext pair, we can compute $y = S^{-1}[c \oplus k_3]$. Now the rest of cipher is just a CipherTwo.

$$c = S[S[S[m \oplus k_0] \oplus k_1] \oplus k_2] \oplus k_3$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b



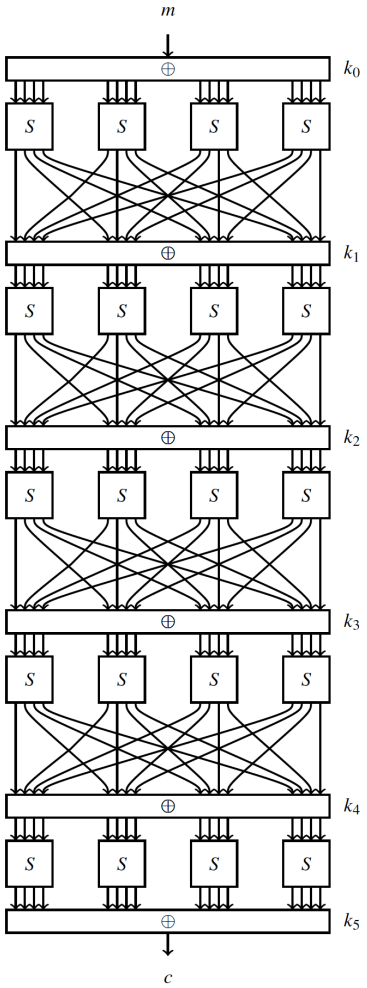
CipherFour

16-bit block cipher, r rounds (r+1 independent round keys)

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b

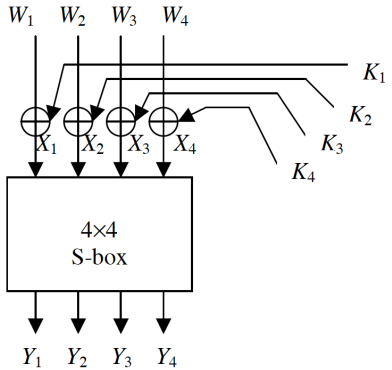
i	0	1	2	3	4	5	6	7
$P[i]$	0	4	8	12	1	5	9	13
i	8	9	10	11	12	13	14	15
$P[i]$	2	6	10	14	3	7	11	15

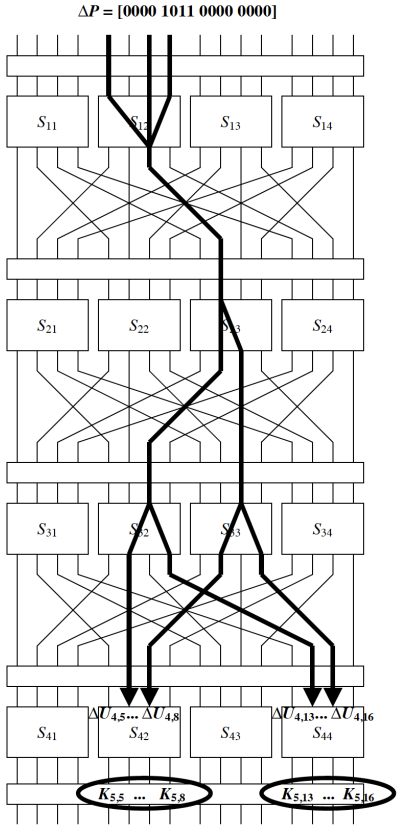
1. Set $u_0 = m$.
2. For $i := 1$ to $r-1$ do:
   a. Combine the round key k_{i-1} with u_{i-1} so that $a_i = u_{i-1} \oplus k_{i-1}$.
   b. Divide a_i into four nibbles $a_i = A_0||\ldots||A_3$.
   c. Compute $S[A_0]||\ldots||S[A_3]$ where $S[\cdot]$ is defined above.
   d. Write $S[A_0]||\ldots||S[A_3]$ as $y_{15}\ldots y_0 = S[A_0]||\ldots||S[A_3]$.
   e. Permute bit y_i to position j according to the permutation $j = P[i]$ defined above.
   f. Set $u_i = y_{15}||y_{11}||\ldots||y_4||y_0$.
3. *(Last round)*
   a. Combine the round key k_{r-1} with u_{r-1} so that $a_r = u_{r-1} \oplus k_{r-1}$.
   b. Divide a_r into four nibbles $a_r = A_0||\ldots||A_3$.
   c. Compute $S[A_0]||\ldots||S[A_3]$ where $S[\cdot]$ is defined above.
   d. Write $S[A_0]||\ldots||S[A_3]$ as $y = y_{15}\ldots y_0 = S[A_0]||\ldots||S[A_3]$.
   e. Output $y \oplus k_r$ as ciphertext.



One-round Characteristic

- S-box: $(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \longrightarrow^{S} (\beta_1,\beta_2,\beta_3,\beta_4)$
- P-box: $(\beta_1,\beta_2,\beta_3,\beta_4) \longrightarrow^{P} (\gamma_1,\gamma_2,\gamma_3,\gamma_4)$
- Full round: $(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \longrightarrow^{R} (\gamma_1,\gamma_2,\gamma_3,\gamma_4)$
- Iterative characteristic:
  $(0,0,2,0) \longrightarrow^{R} (0,0,2,0)$ with probability 6/16
  $(0,0,2,0) \longrightarrow^{R} (0,0,2,0) \longrightarrow^{R} (0,0,2,0)$ with probability $(6/16)^2$





Differential

- The probability of any given difference occurring at random is 1/16 = 0.06
- Iterative characteristic has too small probability:
  $(0,0,2,0) \longrightarrow^{R} (0,0,2,0) \longrightarrow^{R} (0,0,2,0) \longrightarrow^{R} (0,0,2,0) \longrightarrow^{R} (0,0,2,0)$ $p=(6/16)^4 = 0.02$
- At least three other characteristic have the same start and end differences:
  $(0,0,2,0) \longrightarrow^{R} (0,0,0,2) \longrightarrow^{R} (0,0,0,1) \longrightarrow^{R} (0,0,1,0) \longrightarrow^{R} (0,0,2,0)$ $p= 0.02$
  $(0,0,2,0) \longrightarrow^{R} (0,0,0,2) \longrightarrow^{R} (0,0,1,0) \longrightarrow^{R} (0,0,2,0) \longrightarrow^{R} (0,0,2,0)$ $p= 0.02$
  $(0,0,2,0) \longrightarrow^{R} (0,0,2,0) \longrightarrow^{R} (0,0,0,2) \longrightarrow^{R} (0,0,1,0) \longrightarrow^{R} (0,0,2,0)$ $p= 0.02$
- The attacker is only concerned with the difference in the partially encrypted inputs after four rounds:
  $(0,0,2,0) \longrightarrow^{R} ? \longrightarrow^{R} ? \longrightarrow^{R} ? \longrightarrow^{R} (0,0,2,0)$ $p >= 0.08$
  such structure is called a differential.

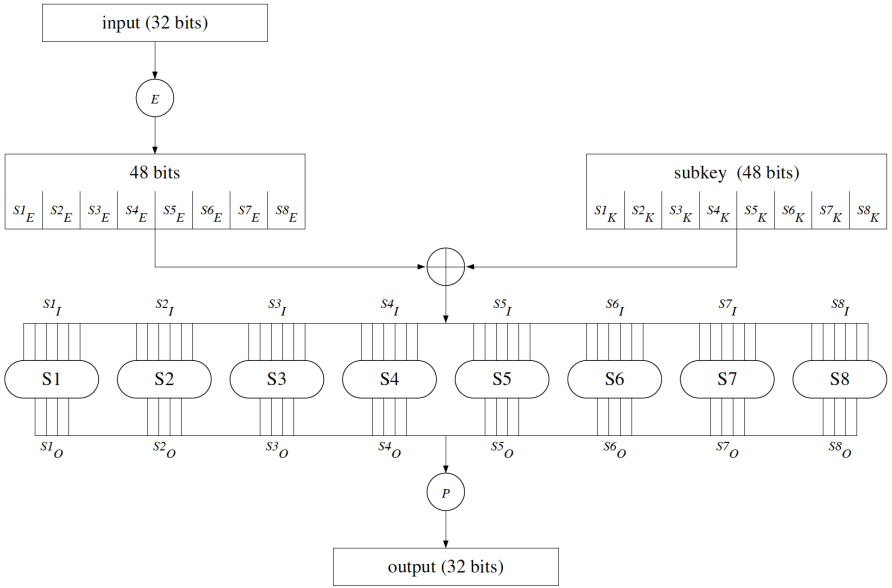
Filtering

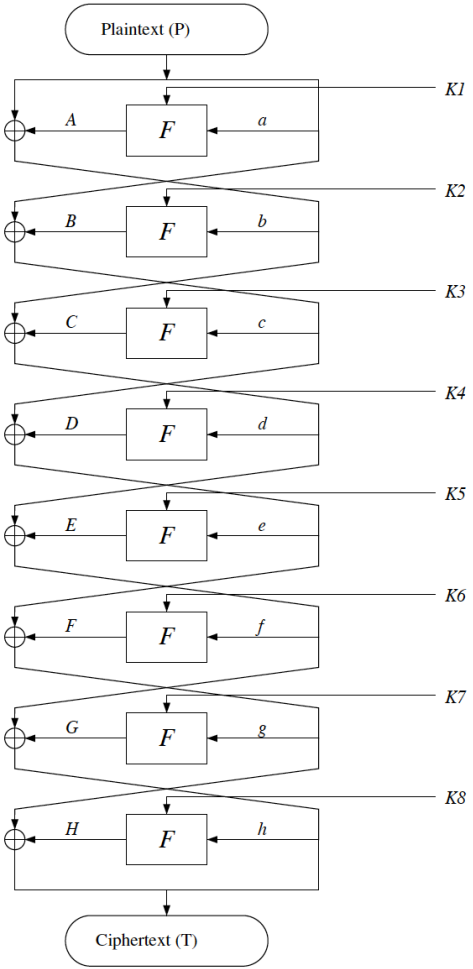
- A pair that follows that characteristic is called a right pair;
- A pair which deviates from the characteristic at some point is called a wrong pair.
- The process of discarding wrong pairs is called filtering and a good filtering technique is essential for the success of many differential attacks.
- Example: 5^{th} round, $(0,0,2,0) \longrightarrow^{S} (0,0,h,0)$, h=1,2,9,a

  for each message pair, the attacker can inspect the corresponding ciphertext pair and immediately determine whether a pair is a wrong pair or, potentially, a right pair.

Attack DES variants

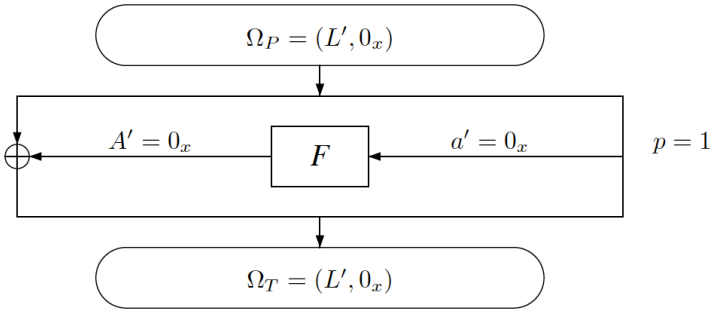
- Plaintext (P): after initial permutation
- Ciphertext (T): before final permutation
- Difference: $X' = X \oplus X^*$



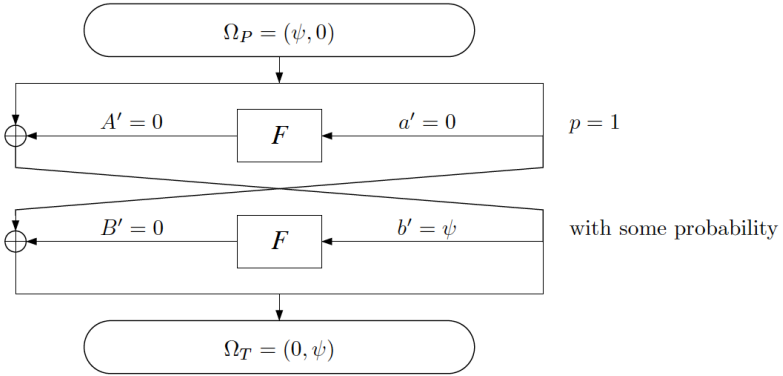


Characteristics

One-round characteristic



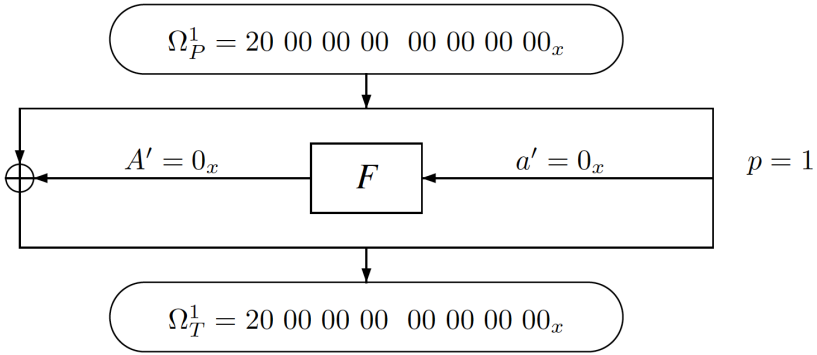
Two-round characteristic

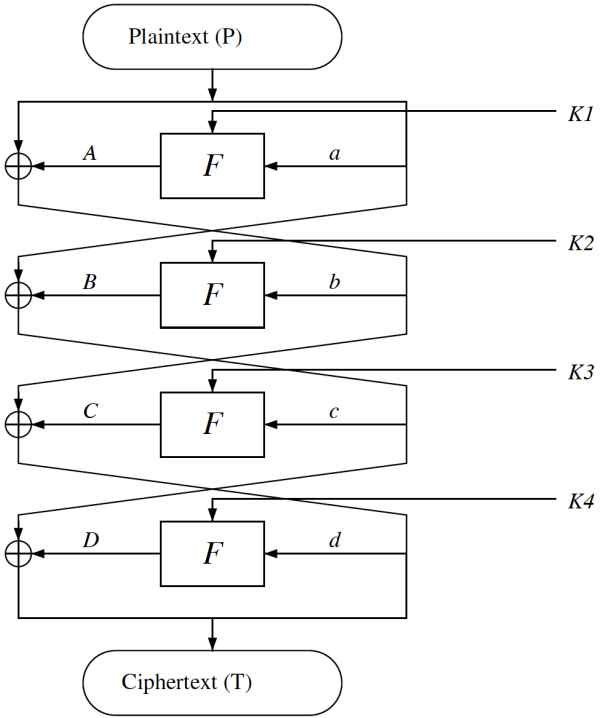


A *n*-round characteristic Ω^1 can be concatenated with a *m*-round characteristic Ω^2 if Ω^1_T equals the swapped value of the two halves of Ω^2_P

Attack DES reduced to 4 rounds (1)

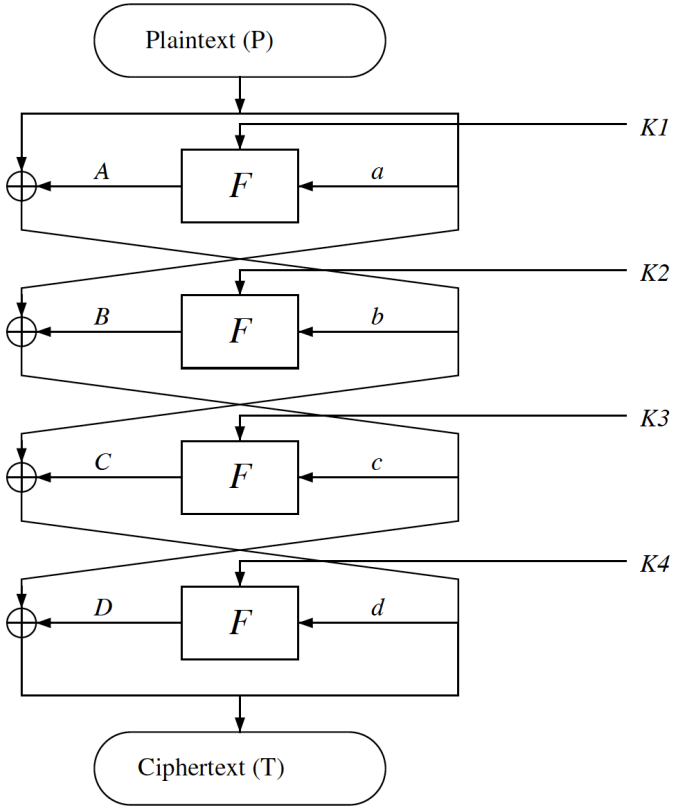
In this attack we used the following one-round characteristic Ω^1 with probability 1, where in the second round (if added) b′ = 20 00 00 00_x:





Attack DES reduced to 4 rounds (2)

- $a' = 0$, $A' = 0$
- $b' = 20\ 00\ 00\ 00_x$
- B' (at least 28 bits) = 0
- $d' = T'_R$ (known)
- $D' = B' \oplus T'_L$ (known)
- The corresponding 28 bits of D' are known.
- These 28 bits are the output differences of the S-boxes S2, ..., S8.
- Thus, we know the values S_{Ed}, S^*_{Ed} and S'_{Od} of seven S-boxes in the 4^{th} round.

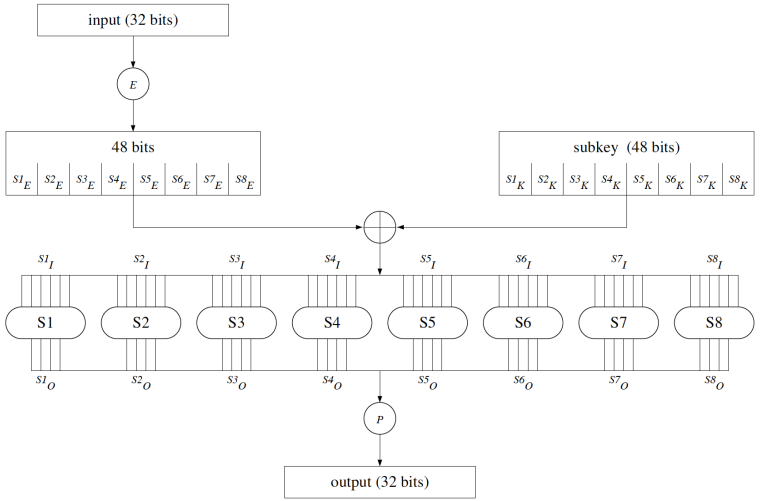


Attack DES reduced to 4 rounds (3)

1. Given four encrypted pairs, use a separated counting procedure for each one of the seven S-boxes in the fourth round.
2. Try all the 64 possible values of S_{Kd} and check whether

$$S(S_{Ed} \oplus S_{Kd}) \oplus S(S_{Ed} \oplus S_{Kd}) = S'_{Od}$$

3. For each key, count the number of pairs for which the test succeeds. The right key value is suggested by all the pairs. The other 63 key values may occur in only some of the pairs.
4. So far we found 7*6 = 42 bits of the subkey of the last round (K4). If the subkeys are calculated via the key scheduling algorithm of DES, these are 42 actual key bits out of the 56 key bits.
5. For the rest missing 14 key bits, we can simply guess them.



THEORY OF S-BOX

Design Criteria of DES S-Boxes

- (S-1) Each S-box has six bits of input and four bits of output.
- (S-2) No output bit of an S-box should be too close to a linear function of the input bits.
- (S-3) If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, each possible 4-bit output is attained once as the middle four input bits range over their 16 possibilities.
- (S-4) If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits.
- (S-5) If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits.
- (S-6) If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same.
- (S-7) For any nonzero 6-bit difference between inputs, no more than eight of the 32 pairs of inputs may result in the same output difference.

How to get DES S-Boxes

- A pool of possible S-boxes was generated according to the design criteria developed thus far;
- These boxes were then ranked according to how efficiently they could be implemented;
- As the process evolved and more constraints were put on the S-boxes, the pool of boxes shrunk and the complexity of the most efficient ones increased.
- In the end there were three S-boxes with the same most-efficient implementation and seven S-boxes with the same second most-efficient implementation.
- “It seems that the eight S-boxes for DES were chosen from this set of ten.”

S-Box and Boolean Functions

- A Boolean function of n variables is a *function on* B^n *into* B*, where* B *is the set* {0, 1}*,* n *is a positive integer; and* B^n *denotes the* n*-fold cartesian product of the set* B *with itself.*
- Let n and m be two positive integers. The functions from B^n to B^m are called (n, m)-*functions*. Such function F being given, the Boolean functions $f_1, \ldots, f_m$ defined, at every $x \in B_n$, by $F(x) = (f_1(x),\ldots,f_m(x))$, are called the *coordinate functions* of F. When the numbers m and n are not specified, (n, m)-functions are called *multioutput Boolean functions*, *vectorial Boolean functions*, or *S-boxes*.

Algebraic Normal Form

Let $f(x)$ be a Boolean function $f : \{0,1\}^n \to \{0,1\}$ that maps n-bit inputs to a single bit of output. We will denote the binary representation of an input x by $x_{n-1}x_{n-2}\ldots x_1x_0$. It is well known that we can write the output of the function as a (unique) multivariate expression in terms of the n input bits:

$$f(x) = \sum_{b\in\{0,1\}^n} A_f(b) x_{n-1}^{b_{n-1}} x_{n-2}^{b_{n-2}} \cdots x_1^{b_1} x_0^{b_0}.$$

(A_f is another boolean function)

Algebraic Degree (AD)

AD(f) = the maximum Hamming weight of b $\in \{0,1\}^n$ for which $A_f(b) = 1$.

Let $f : \mathcal{B}^3 \to \mathcal{B}$ be a Boolean function defined by the following look-up table:

x	0	1	2	3	4	5	6	7
$f(x)$	1	0	1	0	1	0	1	1

The algebraic normal form can be derived as $f(x) = x_2x_1x_0 + x_0 + 1$ and so the algebraic degree $\mathrm{AD}(f)$ is 3.

The algebraic degree of the S-box to be the maximum algebraic degree of the coordinate functions of the S-box.

Non-Linear Degree

- Given an (n,m)-function f with f : $\{0,1\}^n \longrightarrow \{0,1\}^m$, the nonlinear degree of f, denoted by NL(f), is the minimum value of the algebraic degree of all linear combinations of the coordinate functions of f.
- This is a more demanding criterion than the algebraic degree itself and a high value to this quantity would again, at least intuitively, appear to be a desirable attribute.
- Loosely, it implies that not only are individual output bits from the S-box complicated, but so are some simple simple algebraic combinations.

Input-Output Degree

Suppose we have an (n, m)-function f, then we can represent all the input bits as $x_{n-1} \ldots x_0$ and all the output bits as $y_{m-1} \ldots y_0$. We can then consider deriving a multivariate equation that holds over all inputs and has the following form:

$$\sum_{b \in \mathcal{B}^{n+m}} B_f(b) y_{m-1}^{b_{n+m-1}} y_{m-2}^{b_{n+m-2}} \cdots y_1^{b_{n+1}} y_0^{b_n}$$

$$x_{n-1}^{b_{n-1}} x_{n-2}^{b_{n-2}} \cdots x_1^{b_1} x_0^{b_0} = 0.$$

The sum is computed modulo 2 and B_f is a Boolean function on $(m + n)$-bit inputs that sets each coefficient for the 2^{n+m} terms in the summation. If we define d to be equal to the maximum Hamming weight of $b \in \mathcal{B}^{m+n}$ for which $B_f(b) = 1$, then d is termed the *degree* of the multivariate expression.

Relationships between AD, NL, IO

- For any (n,m)-function f,

$$AD(f) \geq NL(f) \geq IO(f)$$

- Bounds on the IO degree depend closely on the size of the input and output:

n	m	Maximum IO degree
4	4	2
6	4	3
8	8	3
16	16	5
32	32	8
64	64	16
128	128	30

Choosing S-Boxes

- S-Box that has the upper bound IO degree;
- S-Box that has highest possible algebraic and non-linear degrees;
- Constructing from math functions v.s. choosing at random.
- Considerations on hardware limitations.

References

[1] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, J. Cryptology. 4 (1991) 3–72. doi:10.1007/BF00630563.

[2] E. Biham, A. Shamir, Differential Cryptanalysis of the Full 16-round DES, in: Advances in Cryptology — CRYPTO' 92, Springer Berlin Heidelberg, Berlin, Heidelberg, 1992: pp. 487–496. doi: 10.1007/3-540-48071-4_34.

[3] D. Coopersmith, The Data Encryption Standard (DES) and its strength against attacks, IBM Journal of Research and Development. 38 (1994) 243–250. doi:10.1147/rd.383.0243.

[4] H.M. Heys, A Tutorial on Linear and Differential Cryptanalysis, Cryptologia. 26 (2002) 189–221. doi:10.1080/0161-110291890885.

[5] E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, (2009) 1–188.

[6] Y. Crama, P.L. Hammer, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, 2010.

[7] L.R. Knudsen, M.J.B. Robshaw, The Block Cipher Companion, Springer Publishing Company, Incorporated, 2011.

[8] H. Feistel, Cryptography and Computer Privacy, Scientific American. 228 (1973) 15–23.